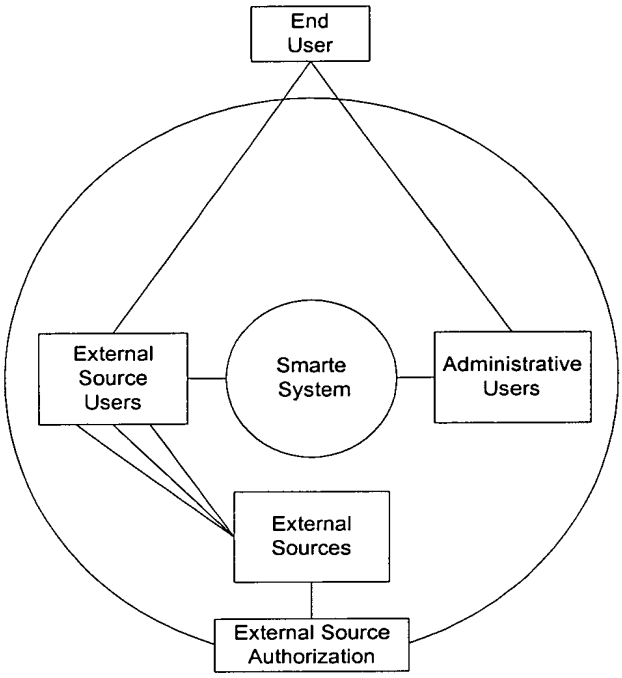
End User
External Source Users
Smarte System
Administrative Users
External Sources
External Source Authorization

FIG. 1

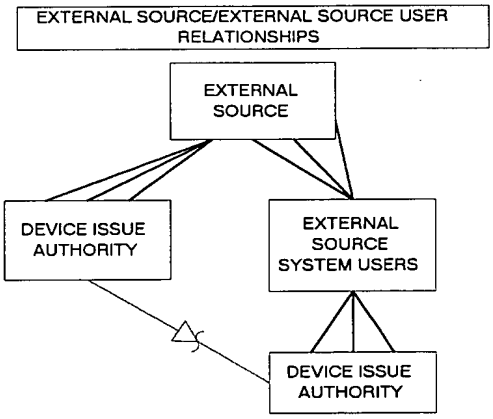
EXTERNAL SOURCE/EXTERNAL SOURCE USER RELATIONSHIPS
EXTERNAL SOURCE
DEVICE ISSUE AUTHORITY
EXTERNAL SOURCE SYSTEM USERS
DEVICE ISSUE AUTHORITY

FIG. 2

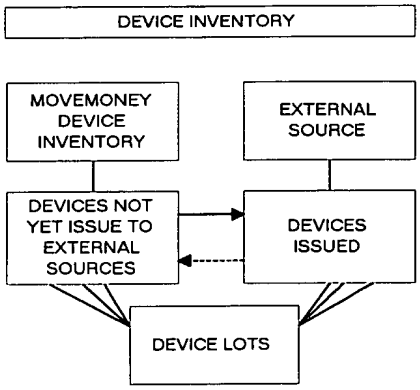

FIG. 3

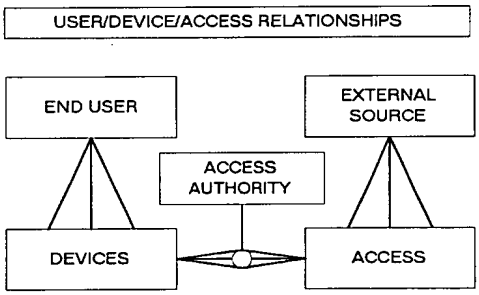

FIG. 4

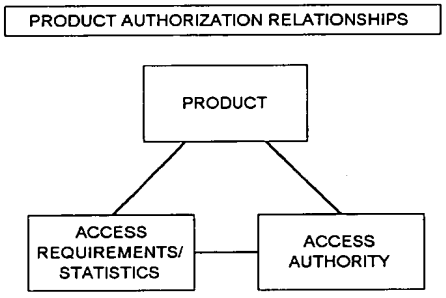

FIG. 5

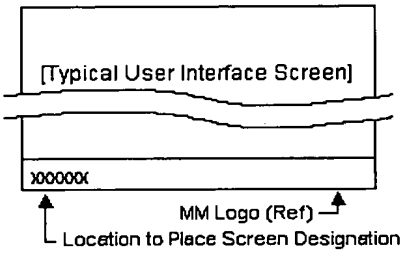

FIG. 6

Page 2 of 32

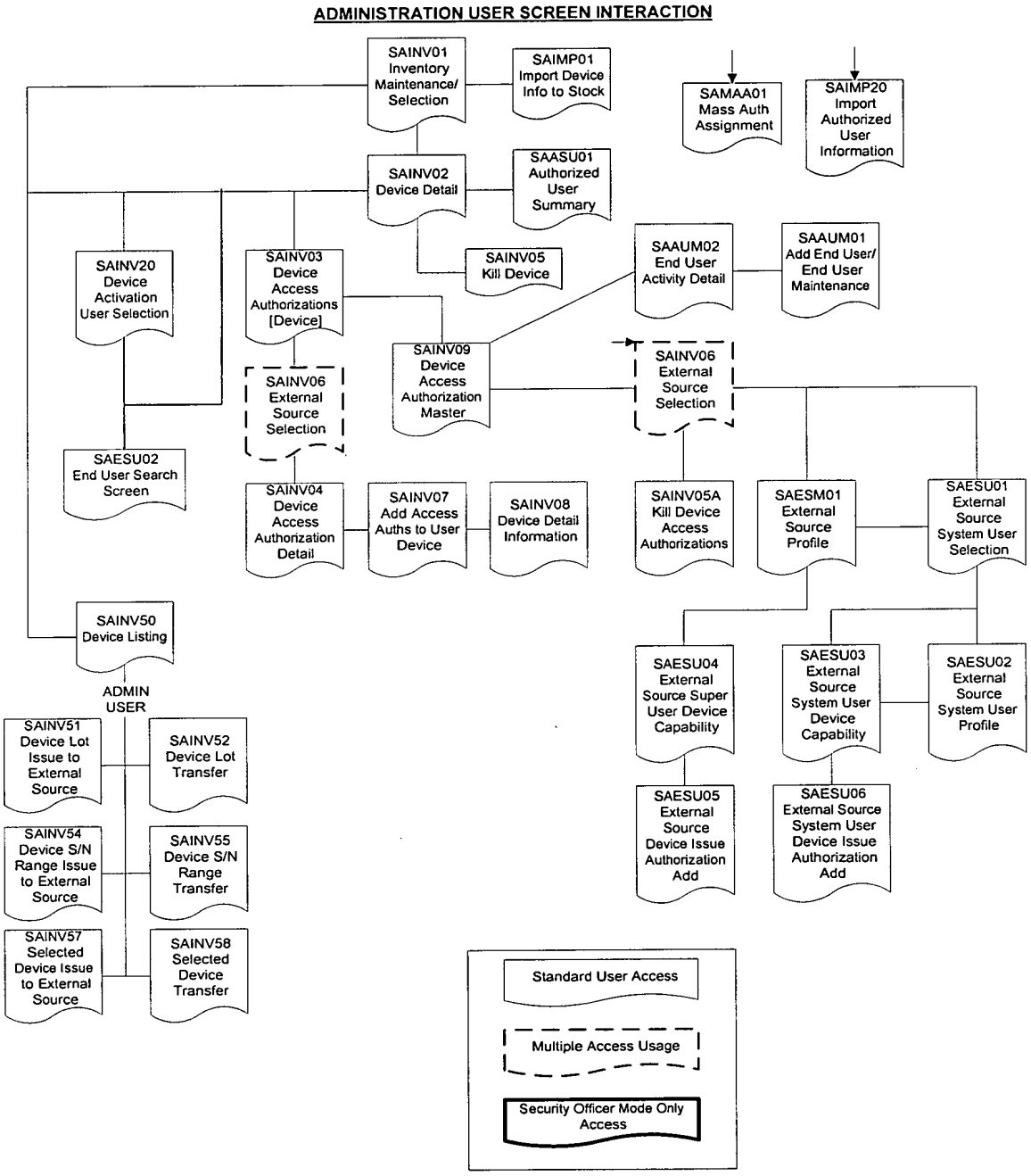
ADMINISTRATION USER SCREEN INTERACTION
SAINV01 Inventory Maintenance/ Selection
SAIMP01 Import Device Info to Stock
SAMAA01 Mass Auth Assignment
SAIMP20 Import Authorized User Information
SAINV02 Device Detail
SAASU01 Authorized User Summary
SAINV20 Device Activation User Selection
SAINV03 Device Access Authorizations [Device]
SAINV05 Kill Device
SAAUM02 End User Activity Detail
SAAUM01 Add End User/ End User Maintenance
SAINV09 Device Access Authorization Master
SAINV06 External Source Selection
SAINV06 External Source Selection
SAESU02 End User Search Screen
SAINV04 Device Access Authorization Detail
SAINV07 Add Access Auths to User Device
SAINV08 Device Detail Information
SAINV05A Kill Device Access Authorizations
SAESM01 External Source Profile
SAESU01 External Source System User Selection
SAINV50 Device Listing
ADMIN USER
SAESU04 External Source Super User Device Capability
SAESU03 External Source System User Device Capability
SAESU02 External Source System User Profile
SAINV51 Device Lot Issue to External Source
SAINV52 Device Lot Transfer
SAESU05 External Source Device Issue Authorization Add
SAESU06 External Source System User Device Issue Authorization Add
SAINV54 Device S/N Range Issue to External Source
SAINV55 Device S/N Range Transfer
SAINV57 Selected Device Issue to External Source
SAINV58 Selected Device Transfer
Standard User Access
Multiple Access Usage
Security Officer Mode Only Access

FIG. 7

EXTERNAL SOURCE USER SCREEN INTERACTION

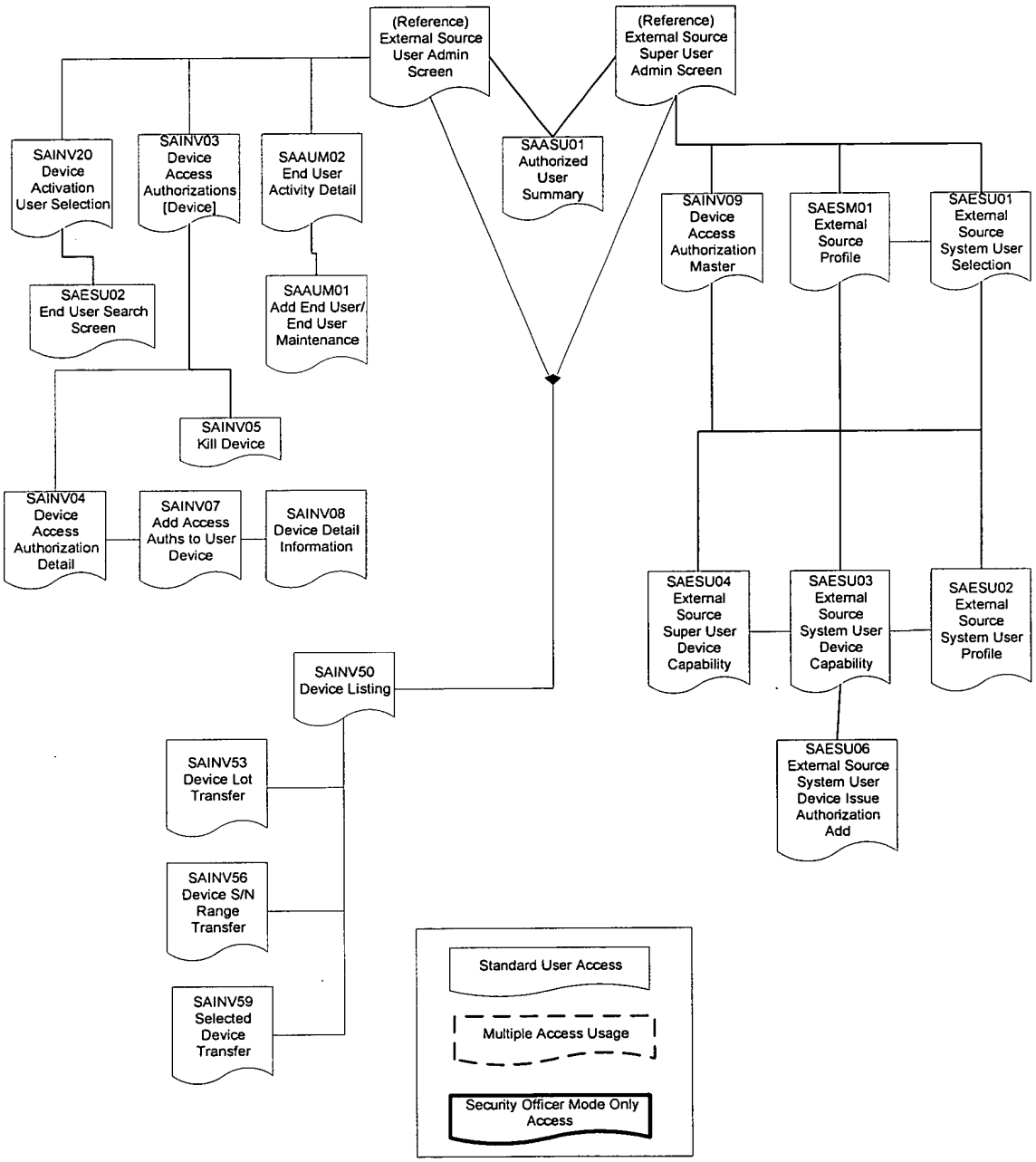

FIG. 8

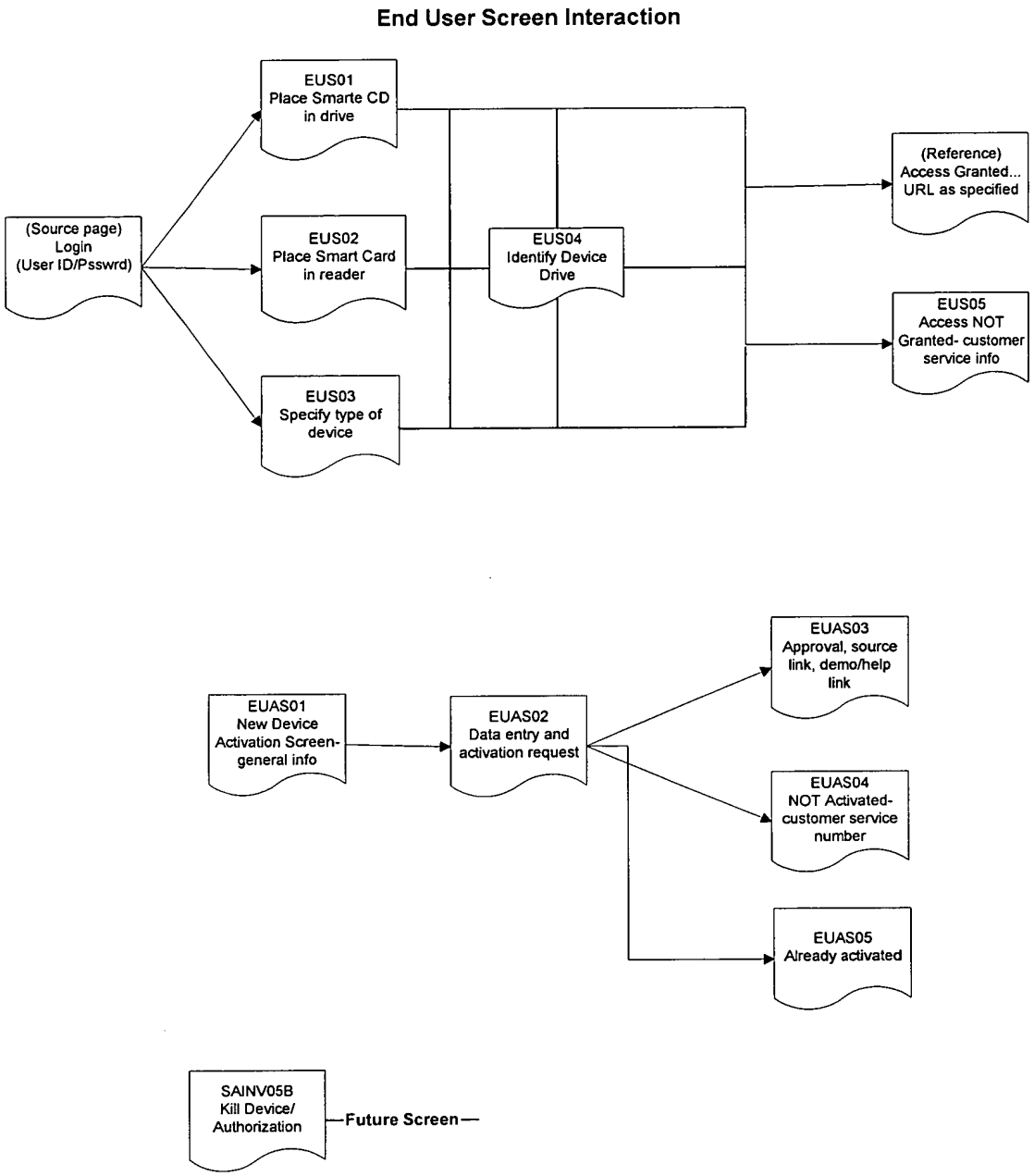

FIG. 9

EFS ID: 1552569

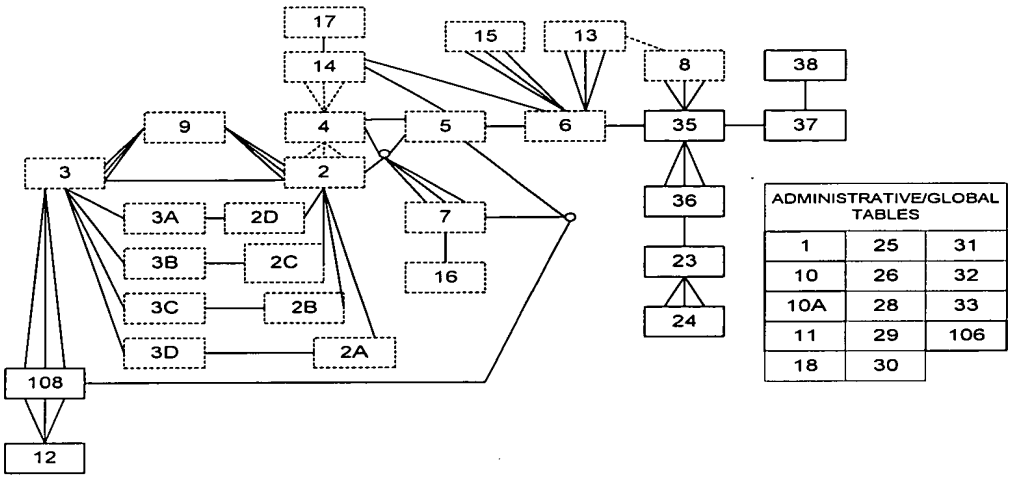

FIG. 10

1	Smarte Authentication System Administration Data		14	Smarte Auth External Source/Auth User Cross Ref
2	Smarte Authentication User Device Master		15	Smarte Auth External Source Device Control Auth
2A	Smarte Authentication Device Specific (Smarte CD)		16	Smarte Authentication Device Auth Overrides
2B	Smarte Authentication Device Specific (Smart Card)		17	Smarte Authentication ES Based End User Detail
2C	Smarte Authentication Device Specific (RSA Token)		18	System Administration Data
2D	Smarte Auth Device Specific (Secure Comp. Token)		23	Identifier Type Master
3	Smarte Authentication Device Inventory Master		24	Identifier Type Master – List Specific
3A	Smarte Auth Device Inventory Specific (Smarte CD)		25	Random Question Master
3B	Smarte Auth Device Inventory Specific (Smart Card)		26	General Parameters
3C	Smarte Auth Device Inventory Specific (Smart Card)		28	Activity Master
3D	SA Device Inventory Specific (Secure Comp. Token)		29	Entity Activity Log
4	Smarte Authentication END User Master		30	Telephone Master
5	Smarte Authentication Authorization Master		31	Zip Master
6	Smarte Authentication External Source Master		32	State Master
7	Smarte Authentication External Source Device		33	Time Zone Master
8	Smarte Auth External Source User Device Issue Auth		35	User Master
9	Smarte Authentication Device Lot Master		36	Identifier Master (User)
10	Smarte Authentication Device Access Log		37	User Block Details
10A	Smarte Authentication Device Access Log ARCHIVE		38	Administration Users Master
11	Smarte Authentication Specific System Activity Log		106	TMP RECORD STORE: MoveMoney Identifier Master
12	Smarte Authentication Product Master		108	Smarte Authentication Product/Device Cross Reference
13	Smarte Auth External Source Device Issue Authority			

FIG. 11

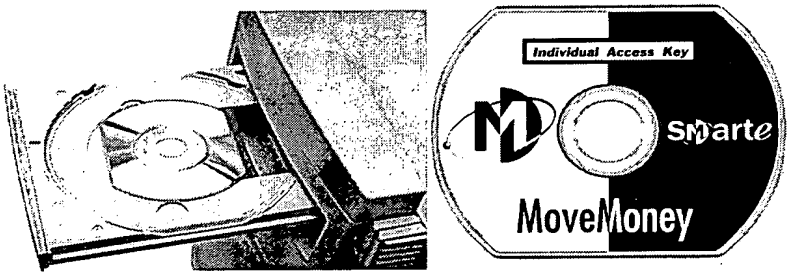

FIG. 12

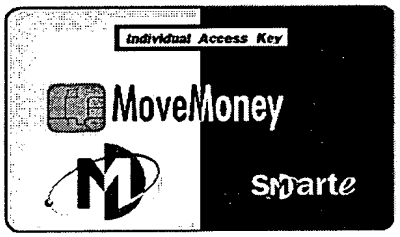

FIG. 13

FIG. 14

Docket No. 2003-0743

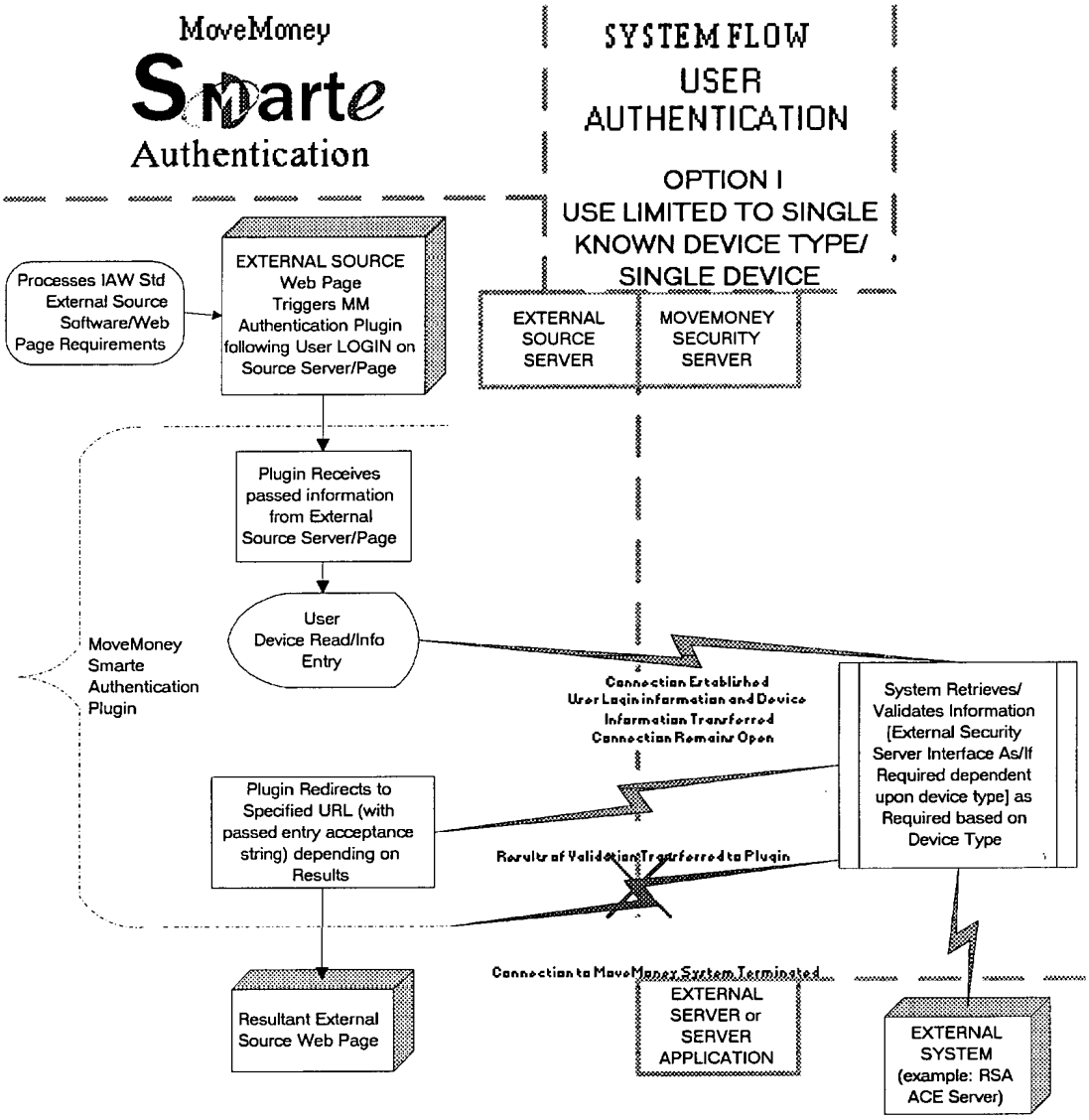
MoveMoney
Smarte
Authentication
SYSTEM FLOW
USER
AUTHENTICATION
OPTION I
USE LIMITED TO SINGLE
KNOWN DEVICE TYPE/
SINGLE DEVICE
EXTERNAL
SOURCE
SERVER
MOVEMONEY
SECURITY
SERVER
Processes IAW Std
External Source
Software/Web
Page Requirements
EXTERNAL SOURCE
Web Page
Triggers MM
Authentication Plugin
following User LOGIN on
Source Server/Page
Plugin Receives
passed information
from External
Source Server/Page
User
Device Read/Info
Entry
MoveMoney
Smarte
Authentication
Plugin
Connection Established
User Login information and Device
Information Transferred
Connection Remains Open
System Retrieves/
Validates Information
(External Security
Server Interface As/If
Required dependent
upon device type] as
Required based on
Device Type
Plugin Redirects to
Specified URL (with
passed entry acceptance
string) depending on
Results
Results of Validation Transferred to Plugin
Connection to MoveMoney System Terminated
Resultant External
Source Web Page
EXTERNAL
SERVER or
SERVER
APPLICATION
EXTERNAL
SYSTEM
(example: RSA
ACE Server)

FIG. 15

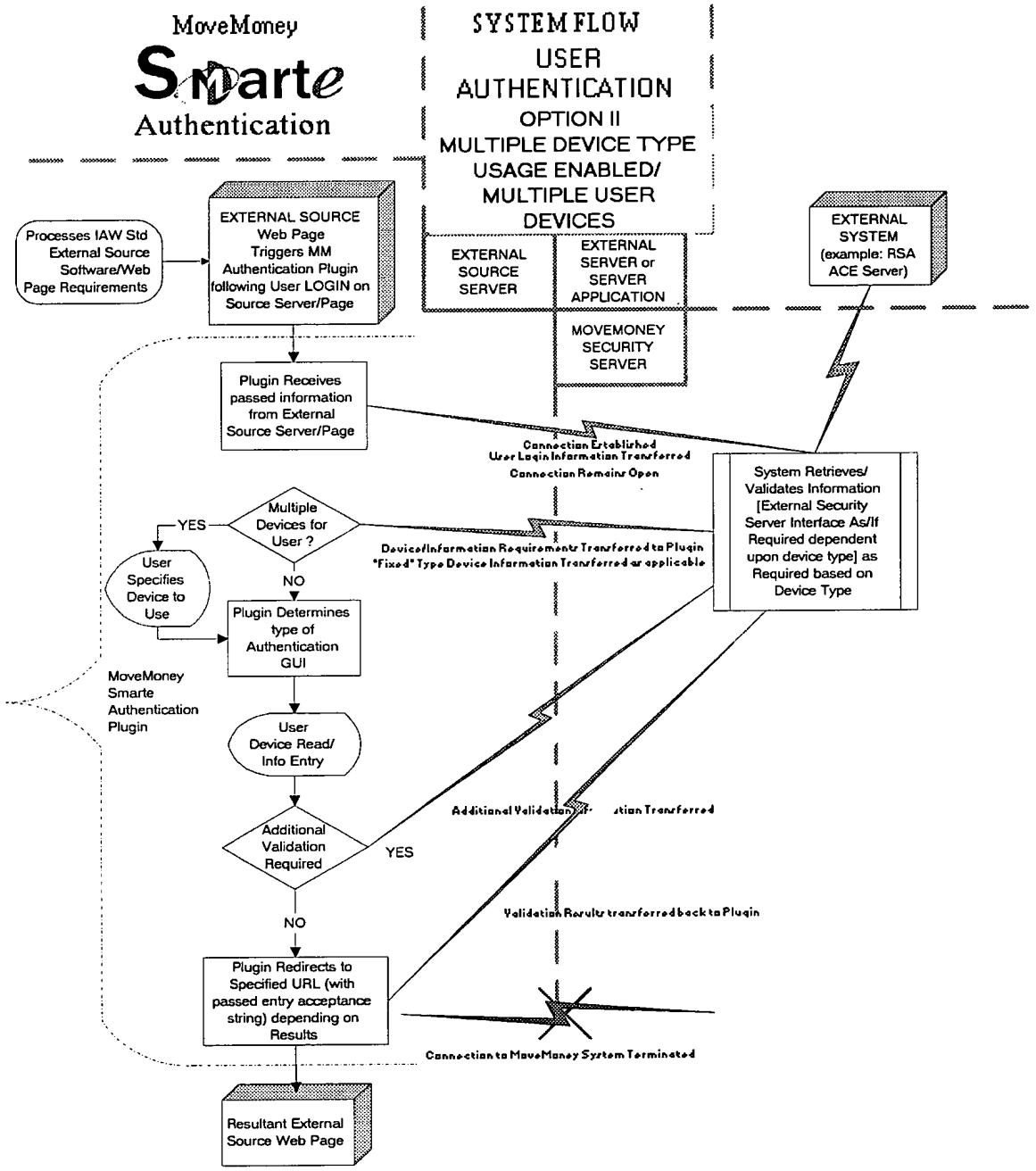
MoveMoney
Smarte
Authentication
SYSTEM FLOW
USER AUTHENTICATION
OPTION II
MULTIPLE DEVICE TYPE USAGE ENABLED/ MULTIPLE USER DEVICES
EXTERNAL SOURCE SERVER
EXTERNAL SERVER or SERVER APPLICATION
MOVEMONEY SECURITY SERVER
EXTERNAL SYSTEM (example: RSA ACE Server)
Processes IAW Std External Source Software/Web Page Requirements
EXTERNAL SOURCE Web Page Triggers MM Authentication Plugin following User LOGIN on Source Server/Page
Plugin Receives passed information from External Source Server/Page
Connection Established
User Login Information Transferred
Connection Remains Open
System Retrieves/ Validates Information [External Security Server Interface As/If Required dependent upon device type] as Required based on Device Type
Multiple Devices for User ?
YES
NO
User Specifies Device to Use
Device/Information Requirements Transferred to Plugin
"Fixed" Type Device Information Transferred as applicable
Plugin Determines type of Authentication GUI
MoveMoney Smarte Authentication Plugin
User Device Read/ Info Entry
Additional Validation Required
YES
NO
Additional Validation Information Transferred
Validation Results transferred back to Plugin
Plugin Redirects to Specified URL (with passed entry acceptance string) depending on Results
Connection to MoveMoney System Terminated
Resultant External Source Web Page

FIG. 16

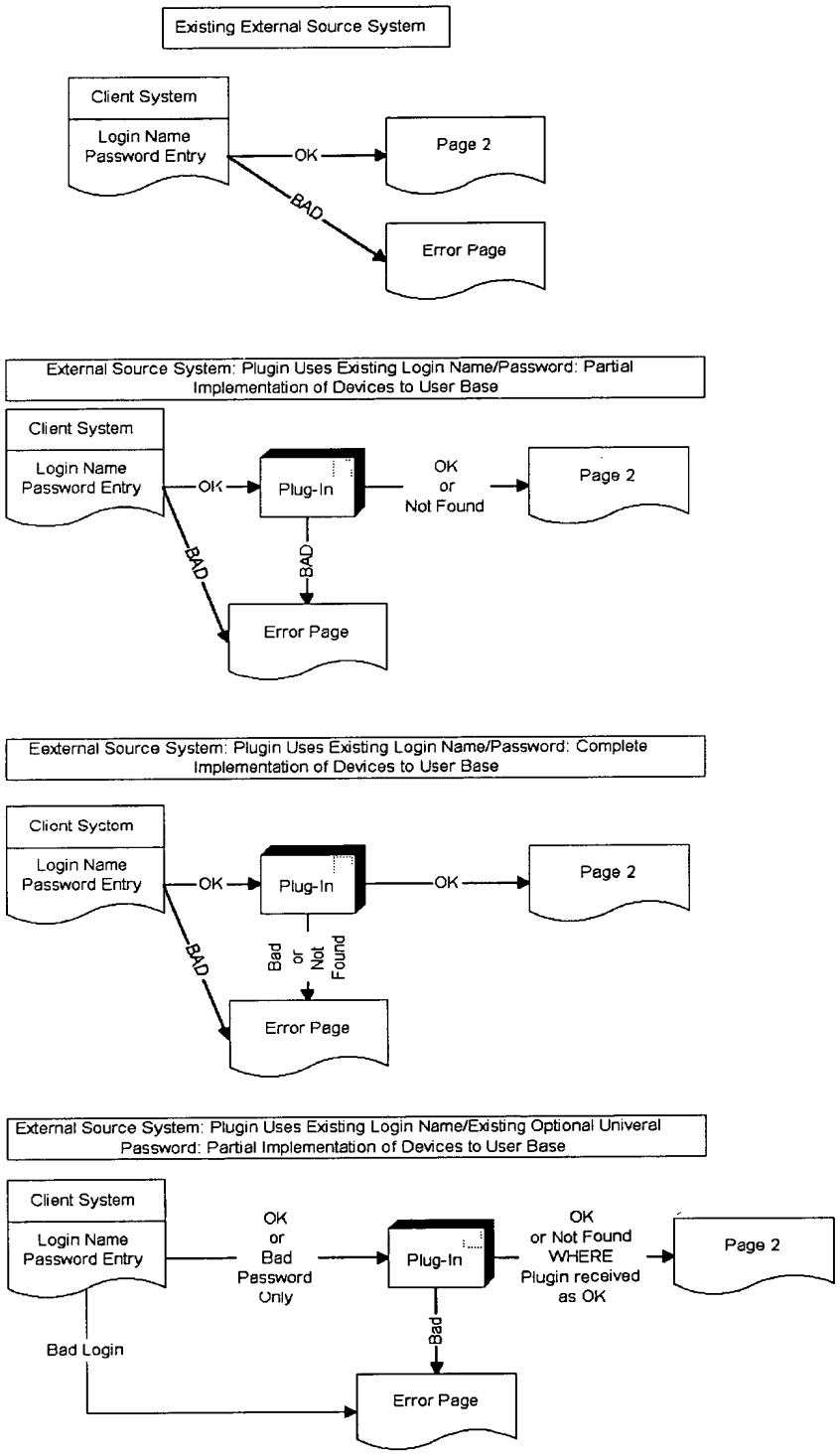
Existing External Source System
Client System
Login Name
Password Entry
OK
BAD
Page 2
Error Page
External Source System: Plugin Uses Existing Login Name/Password: Partial Implementation of Devices to User Base
Client System
Login Name
Password Entry
OK
Plug-In
OK
or
Not Found
Page 2
BAD
BAD
Error Page
Eexternal Source System: Plugin Uses Existing Login Name/Password: Complete Implementation of Devices to User Base
Client Systom
Login Name
Password Entry
OK
Plug-In
OK
Page 2
BAD
Bad
or
Not
Found
Error Page
External Source System: Plugin Uses Existing Login Name/Existing Optional Univeral Password: Partial Implementation of Devices to User Base
Client System
Login Name
Password Entry
OK
or
Bad
Password
Only
Plug-In
OK
or Not Found
WHERE
Plugin received
as OK
Page 2
Bad Login
Bad
Error Page

FIG. 17

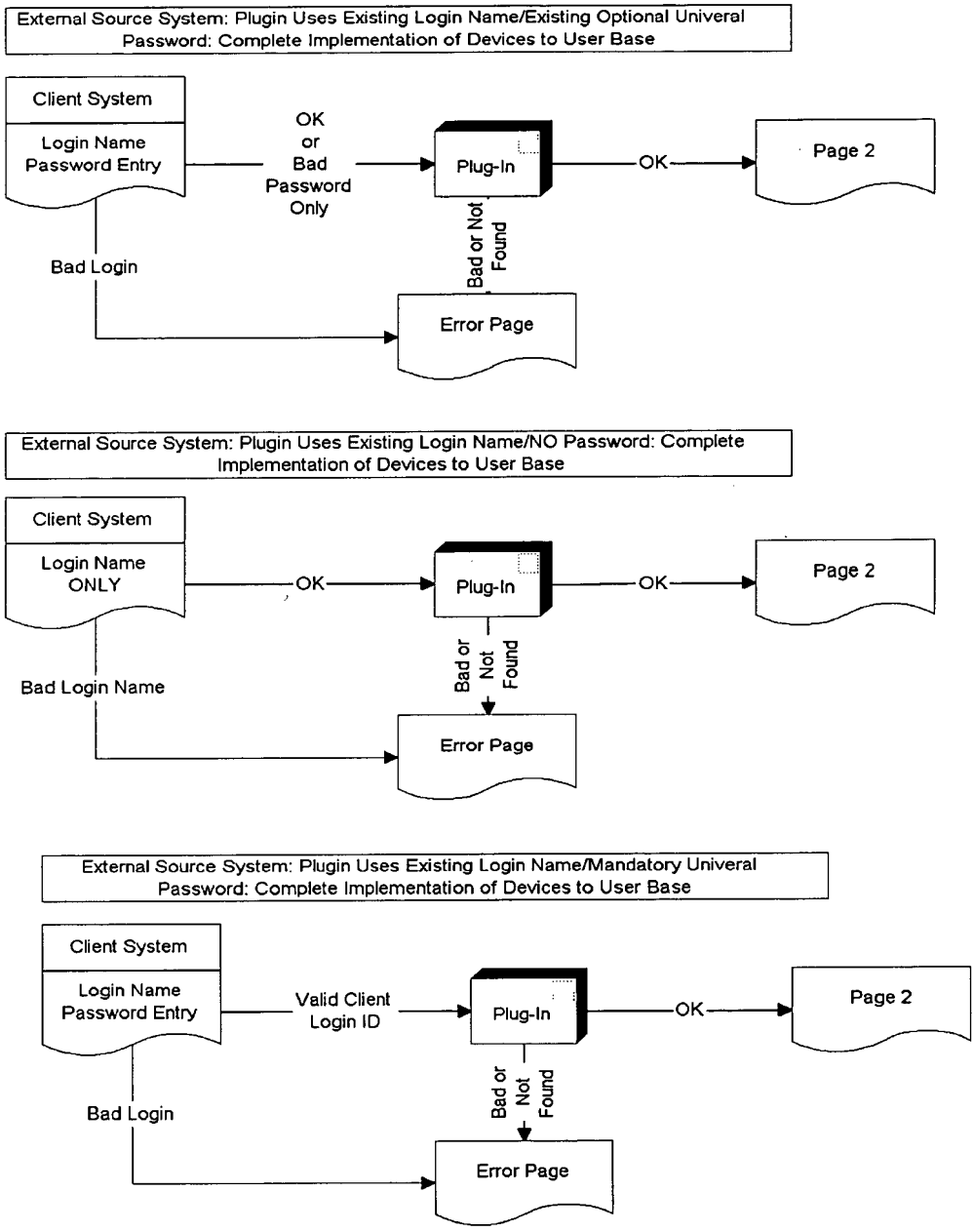
External Source System: Plugin Uses Existing Login Name/Existing Optional Univeral Password: Complete Implementation of Devices to User Base
Client System
Login Name Password Entry
OK or Bad Password Only
Plug-In
OK
Page 2
Bad or Not Found
Bad Login
Error Page
External Source System: Plugin Uses Existing Login Name/NO Password: Complete Implementation of Devices to User Base
Client System
Login Name ONLY
OK
Plug-In
OK
Page 2
Bad or Not Found
Bad Login Name
Error Page
External Source System: Plugin Uses Existing Login Name/Mandatory Univeral Password: Complete Implementation of Devices to User Base
Client System
Login Name Password Entry
Valid Client Login ID
Plug-In
OK
Page 2
Bad or Not Found
Bad Login
Error Page

FIG. 18

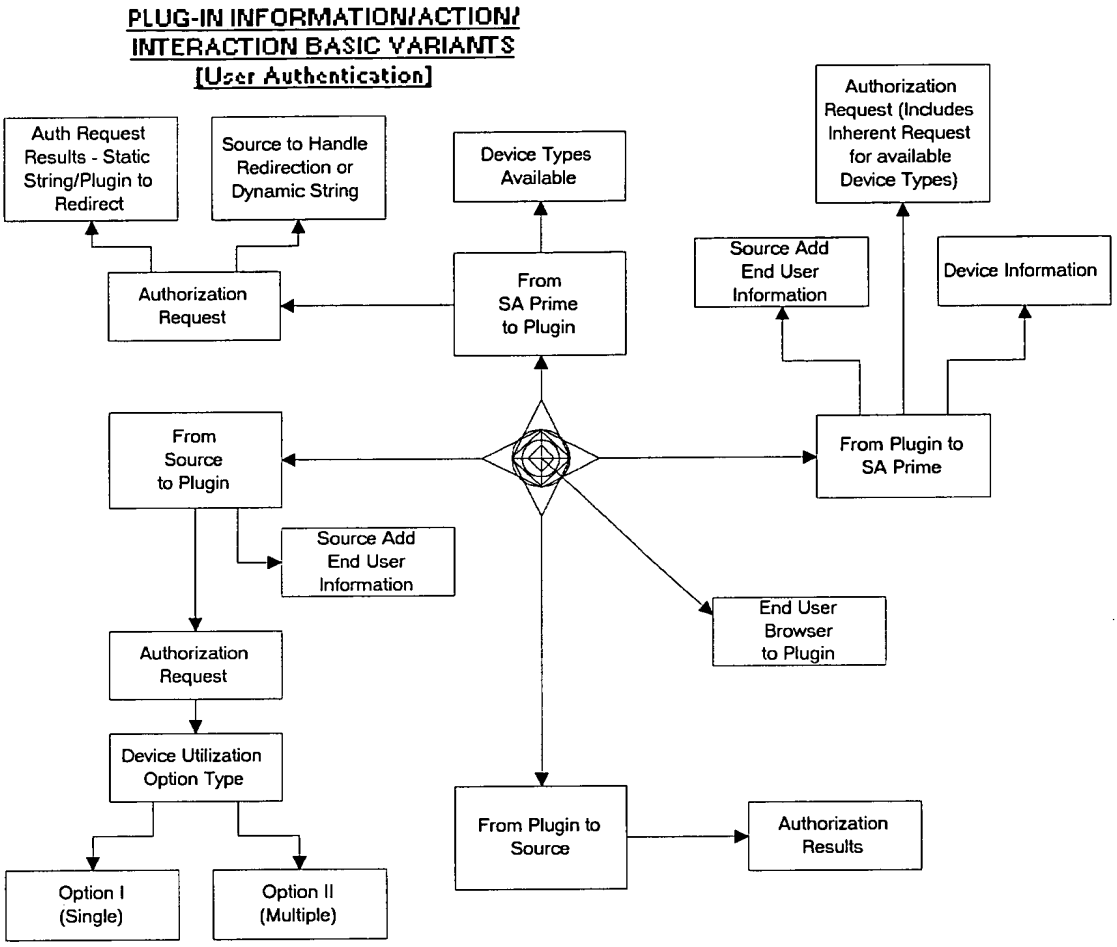
PLUG-IN INFORMATION/ACTION/
INTERACTION BASIC VARIANTS
[User Authentication]
Auth Request Results - Static String/Plugin to Redirect
Source to Handle Redirection or Dynamic String
Device Types Available
Authorization Request (Includes Inherent Request for available Device Types)
Authorization Request
From SA Prime to Plugin
Source Add End User Information
Device Information
From Source to Plugin
From Plugin to SA Prime
Source Add End User Information
End User Browser to Plugin
Authorization Request
Device Utilization Option Type
From Plugin to Source
Authorization Results
Option I (Single)
Option II (Multiple)

FIG. 19

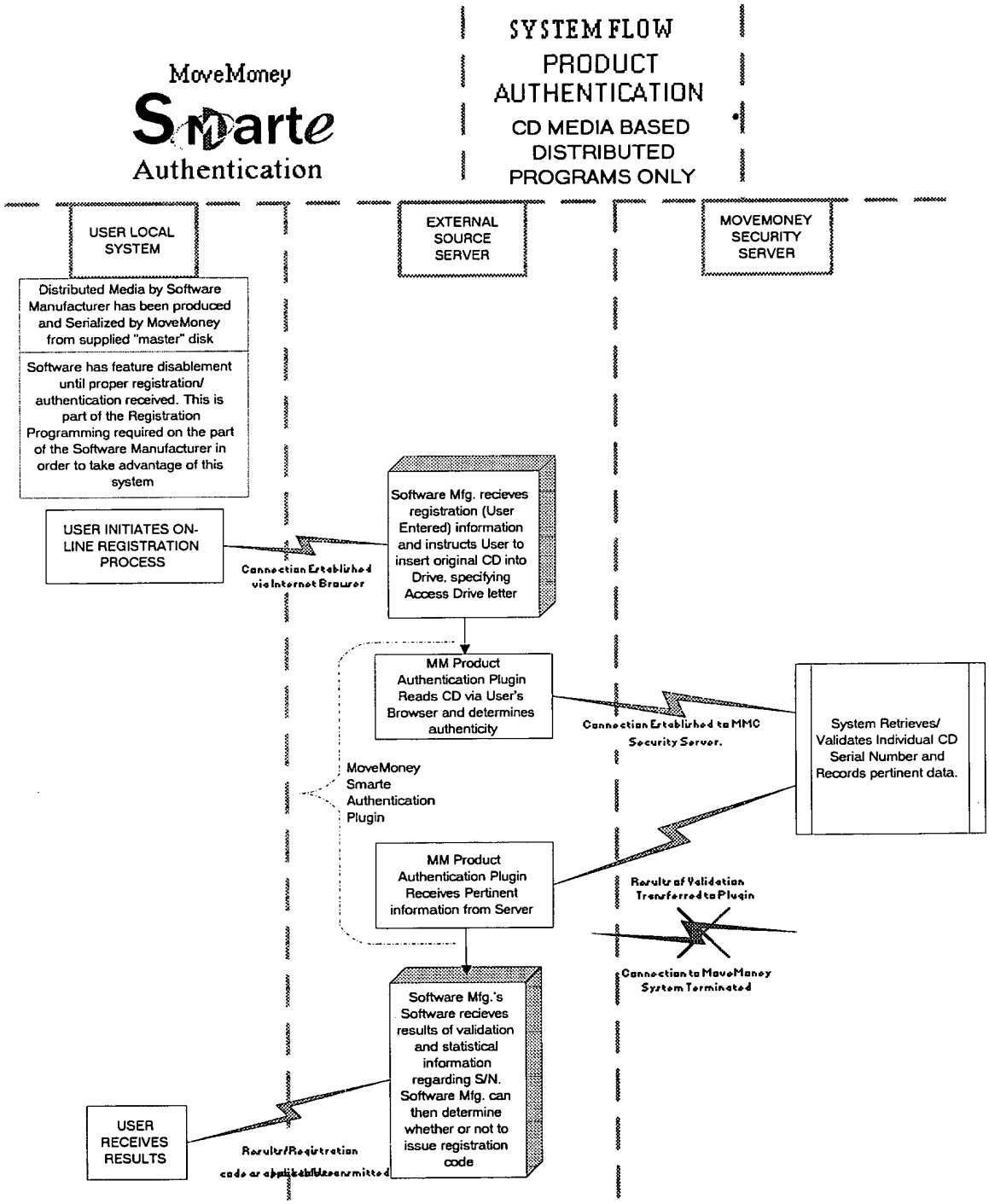
MoveMoney
Smarte
Authentication
SYSTEM FLOW
PRODUCT
AUTHENTICATION
CD MEDIA BASED
DISTRIBUTED
PROGRAMS ONLY
USER LOCAL SYSTEM
EXTERNAL SOURCE SERVER
MOVEMONEY SECURITY SERVER
Distributed Media by Software Manufacturer has been produced and Serialized by MoveMoney from supplied "master" disk
Software has feature disablement until proper registration/ authentication received. This is part of the Registration Programming required on the part of the Software Manufacturer in order to take advantage of this system
USER INITIATES ON-LINE REGISTRATION PROCESS
Connection Established via Internet Browser
Software Mfg. recieves registration (User Entered) information and instructs User to insert original CD into Drive, specifying Access Drive letter
MM Product Authentication Plugin Reads CD via User's Browser and determines authenticity
Connection Established to MMC Security Server.
System Retrieves/ Validates Individual CD Serial Number and Records pertinent data.
MoveMoney Smarte Authentication Plugin
MM Product Authentication Plugin Receives Pertinent information from Server
Results of Validation Transferred to Plugin
Connection to MoveMoney System Terminated
Software Mfg.'s Software recieves results of validation and statistical information regarding S/N. Software Mfg. can then determine whether or not to issue registration code
USER RECEIVES RESULTS
Results/Registration

FIG. 20

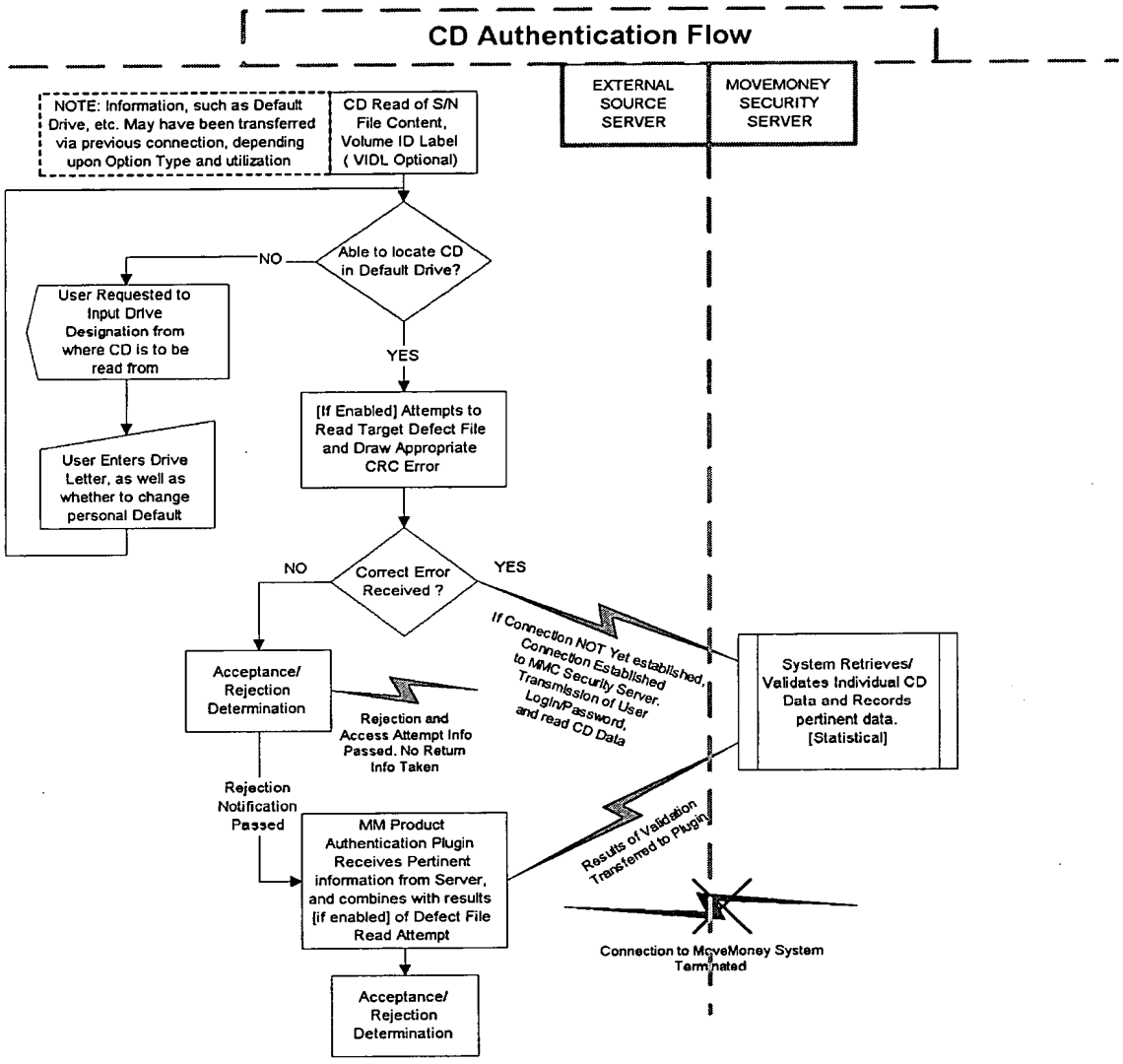
CD Authentication Flow
EXTERNAL SOURCE SERVER
MOVEMONEY SECURITY SERVER
NOTE: Information, such as Default Drive, etc. May have been transferred via previous connection, depending upon Option Type and utilization
CD Read of S/N File Content, Volume ID Label (VIDL Optional)
Able to locate CD in Default Drive?
NO
YES
User Requested to Input Drive Designation from where CD is to be read from
User Enters Drive Letter, as well as whether to change personal Default
[If Enabled] Attempts to Read Target Defect File and Draw Appropriate CRC Error
Correct Error Received ?
NO
YES
If Connection NOT Yet established, Connection Established to MMC Security Server. Transmission of User Login/Password, and read CD Data
System Retrieves/ Validates Individual CD Data and Records pertinent data. [Statistical]
Acceptance/ Rejection Determination
Rejection and Access Attempt Info Passed. No Return Info Taken
Rejection Notification Passed
MM Product Authentication Plugin Receives Pertinent information from Server, and combines with results [if enabled] of Defect File Read Attempt
Results of Validation Transferred to Plugin
Connection to MoveMoney System Terminated
Acceptance/ Rejection Determination

FIG. 21

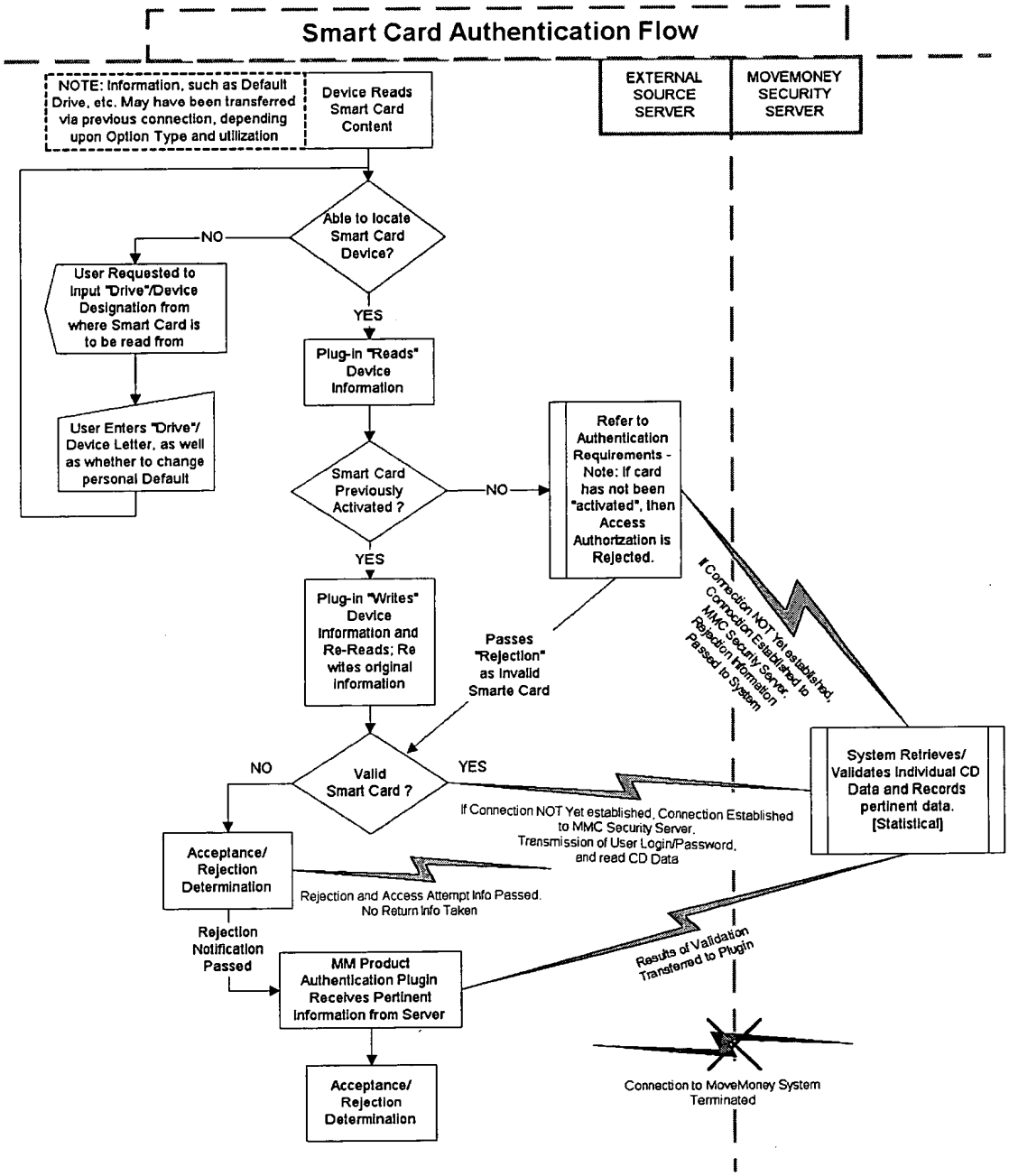
Smart Card Authentication Flow
EXTERNAL SOURCE SERVER
MOVEMONEY SECURITY SERVER
NOTE: Information, such as Default Drive, etc. May have been transferred via previous connection, depending upon Option Type and utilization
Device Reads Smart Card Content
Able to locate Smart Card Device?
NO
YES
User Requested to input "Drive"/Device Designation from where Smart Card is to be read from
User Enters "Drive"/ Device Letter, as well as whether to change personal Default
Plug-in "Reads" Device Information
Smart Card Previously Activated ?
NO
YES
Refer to Authentication Requirements - Note: If card has not been "activated", then Access Authorization is Rejected.
If Connection NOT Yet established, Connection Established to MMC Security Server. Rejection Information Passed to System
Plug-in "Writes" Device Information and Re-Reads; Re wites original information
Passes "Rejection" as Invalid Smarte Card
Valid Smart Card ?
NO
YES
If Connection NOT Yet established, Connection Established to MMC Security Server. Transmission of User Login/Password, and read CD Data
System Retrieves/ Validates Individual CD Data and Records pertinent data. [Statistical]
Acceptance/ Rejection Determination
Rejection and Access Attempt Info Passed. No Return Info Taken
Rejection Notification Passed
MM Product Authentication Plugin Receives Pertinent Information from Server
Results of Validation Transferred to Plugin
Acceptance/ Rejection Determination
Connection to MoveMoney System Terminated

FIG. 22

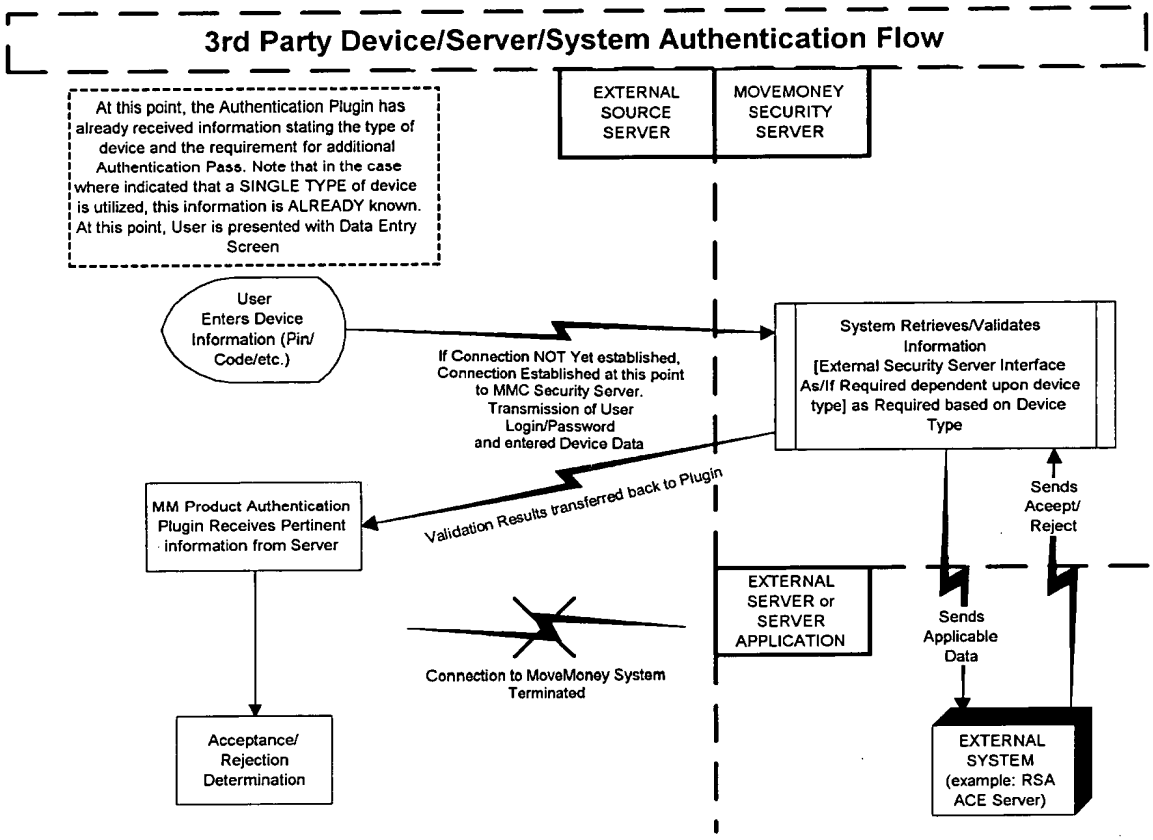
3rd Party Device/Server/System Authentication Flow
EXTERNAL SOURCE SERVER
MOVEMONEY SECURITY SERVER
At this point, the Authentication Plugin has already received information stating the type of device and the requirement for additional Authentication Pass. Note that in the case where indicated that a SINGLE TYPE of device is utilized, this information is ALREADY known. At this point, User is presented with Data Entry Screen
User Enters Device Information (Pin/ Code/etc.)
If Connection NOT Yet established, Connection Established at this point to MMC Security Server. Transmission of User Login/Password and entered Device Data
System Retrieves/Validates Information [External Security Server Interface As/If Required dependent upon device type] as Required based on Device Type
Validation Results transferred back to Plugin
MM Product Authentication Plugin Receives Pertinent information from Server
Sends Aceept/ Reject
EXTERNAL SERVER or SERVER APPLICATION
Sends Applicable Data
Connection to MoveMoney System Terminated
Acceptance/ Rejection Determination
EXTERNAL SYSTEM (example: RSA ACE Server)

FIG. 23

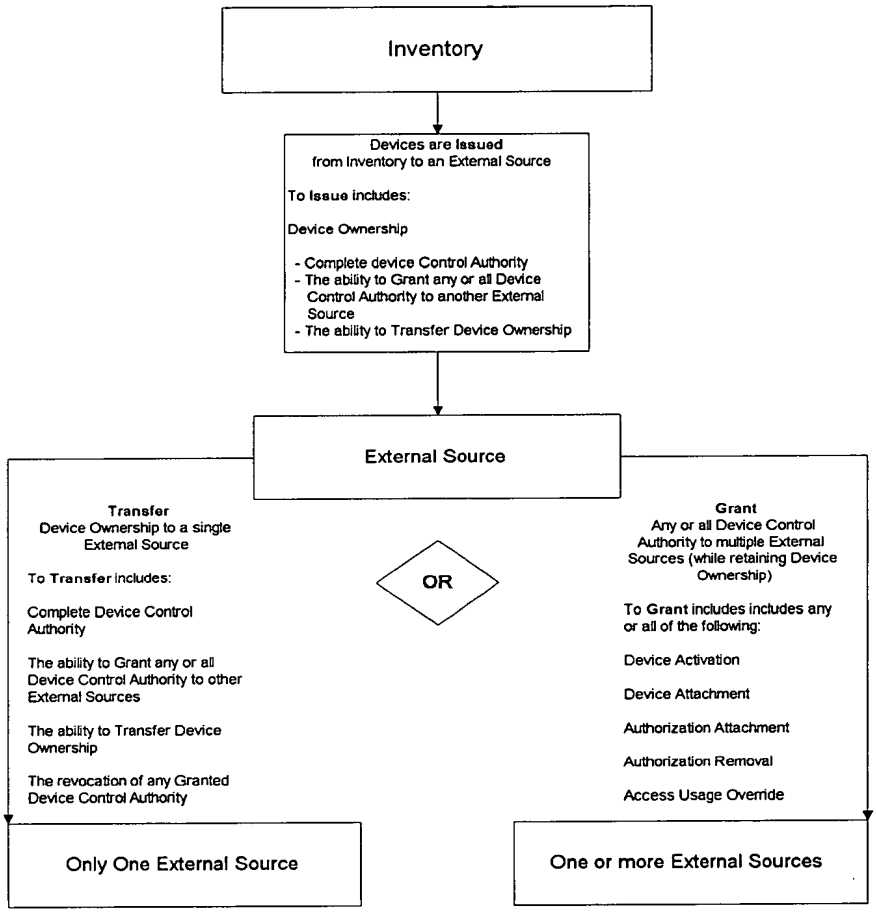
Inventory
Devices are Issued
from Inventory to an External Source
To Issue includes:
Device Ownership
- Complete device Control Authority
- The ability to Grant any or all Device Control Authority to another External Source
- The ability to Transfer Device Ownership
External Source
Transfer
Device Ownership to a single External Source
To Transfer includes:
Complete Device Control Authority
The ability to Grant any or all Device Control Authority to other External Sources
The ability to Transfer Device Ownership
The revocation of any Granted Device Control Authority
OR
Grant
Any or all Device Control Authority to multiple External Sources (while retaining Device Ownership)
To Grant includes includes any or all of the following:
Device Activation
Device Attachment
Authorization Attachment
Authorization Removal
Access Usage Override
Only One External Source
One or more External Sources

FIG. 24

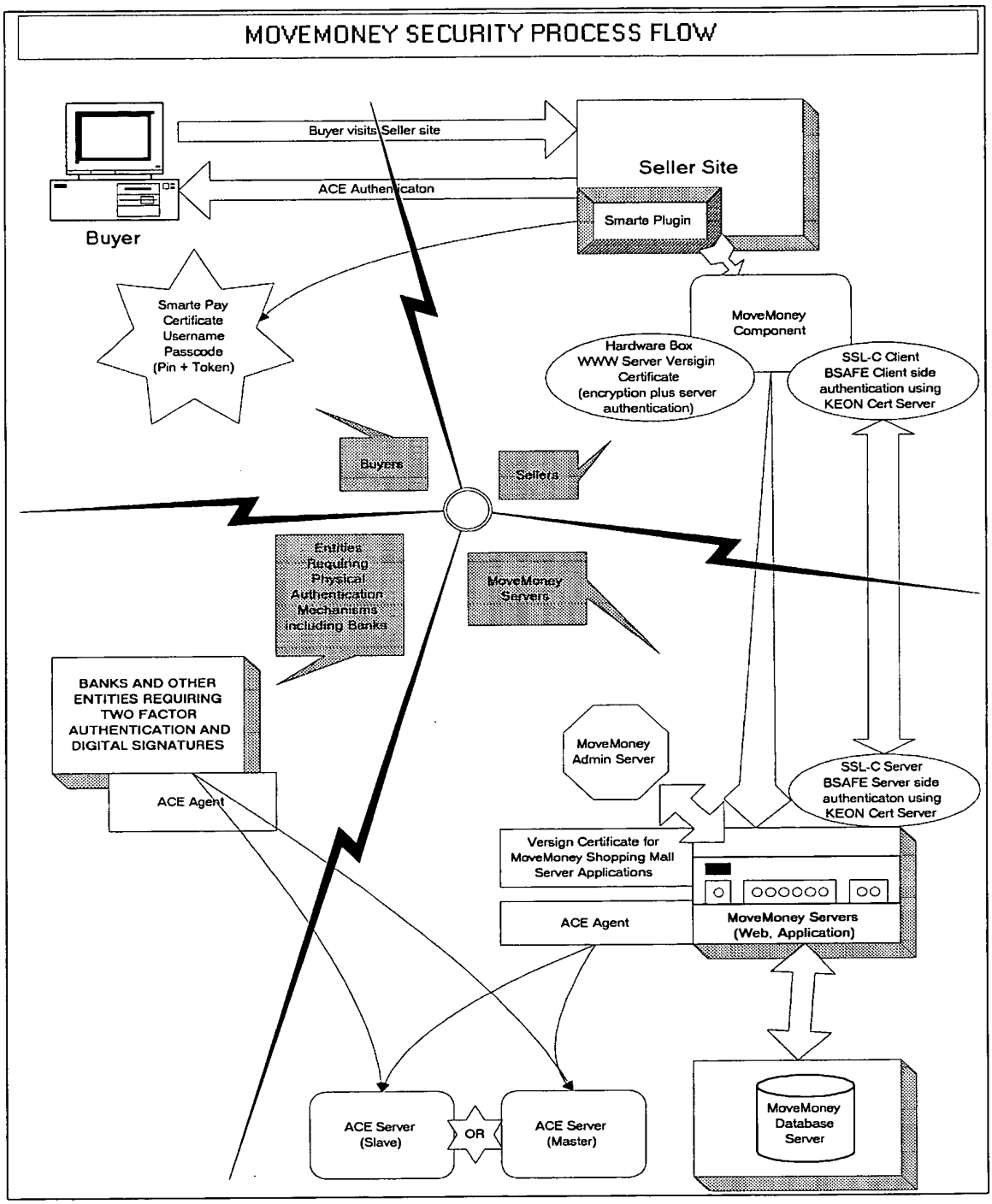
MOVEMONEY SECURITY PROCESS FLOW
Buyer visits Seller site
ACE Authenticaton
Seller Site
Smarte Plugin
Buyer
Smarte Pay
Certificate
Username
Passcode
(Pin + Token)
MoveMoney
Component
Hardware Box
WWW Server Versigin
Certificate
(encryption plus server
authentication)
SSL-C Client
BSAFE Client side
authentication using
KEON Cert Server
Buyers
Sellers
Entities
Requiring
Physical
Authentication
Mechanisms
including Banks
MoveMoney
Servers
BANKS AND OTHER
ENTITIES REQUIRING
TWO FACTOR
AUTHENTICATION AND
DIGITAL SIGNATURES
ACE Agent
MoveMoney
Admin Server
SSL-C Server
BSAFE Server side
authenticaton using
KEON Cert Server
Versign Certificate for
MoveMoney Shopping Mall
Server Applications
ACE Agent
MoveMoney Servers
(Web, Application)
ACE Server
(Slave)
OR
ACE Server
(Master)
MoveMoney
Database
Server

FIG. 25

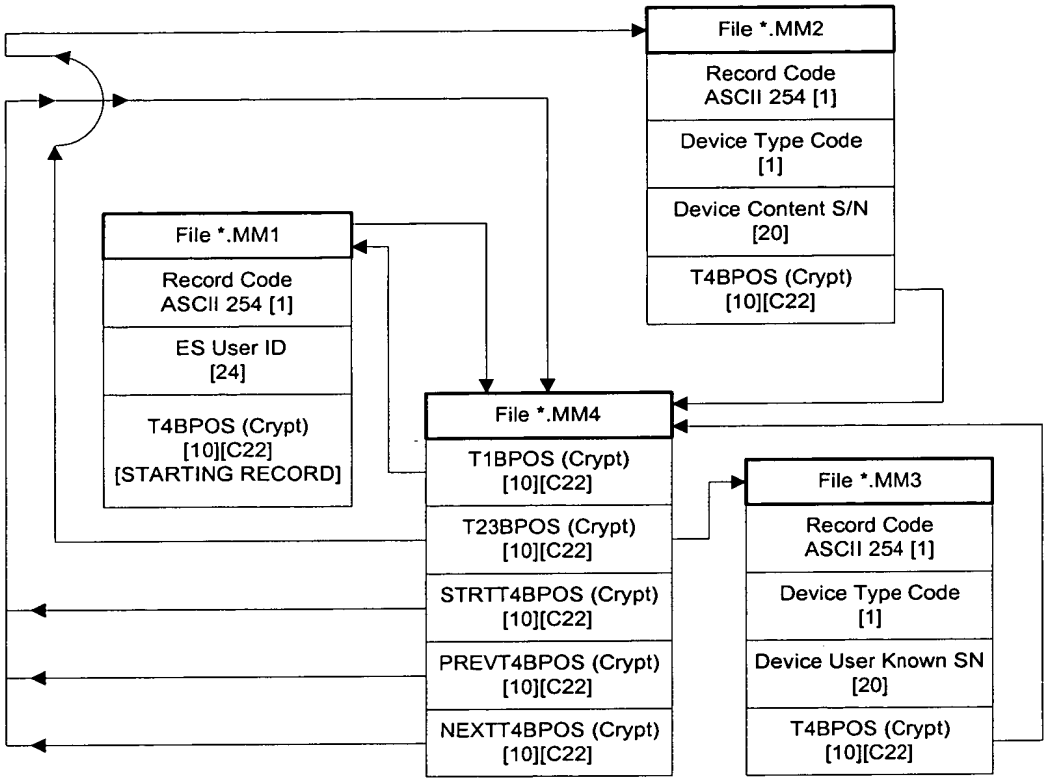
File *.MM2
Record Code ASCII 254 [1]
Device Type Code [1]
Device Content S/N [20]
T4BPOS (Crypt) [10][C22]
File *.MM1
Record Code ASCII 254 [1]
ES User ID [24]
T4BPOS (Crypt) [10][C22] [STARTING RECORD]
File *.MM4
T1BPOS (Crypt) [10][C22]
T23BPOS (Crypt) [10][C22]
STRTT4BPOS (Crypt) [10][C22]
PREVT4BPOS (Crypt) [10][C22]
NEXTT4BPOS (Crypt) [10][C22]
File *.MM3
Record Code ASCII 254 [1]
Device Type Code [1]
Device User Known SN [20]
T4BPOS (Crypt) [10][C22]

FIG. 26

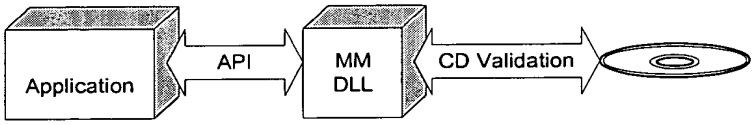
Application
API
MM DLL
CD Validation

FIG. 27

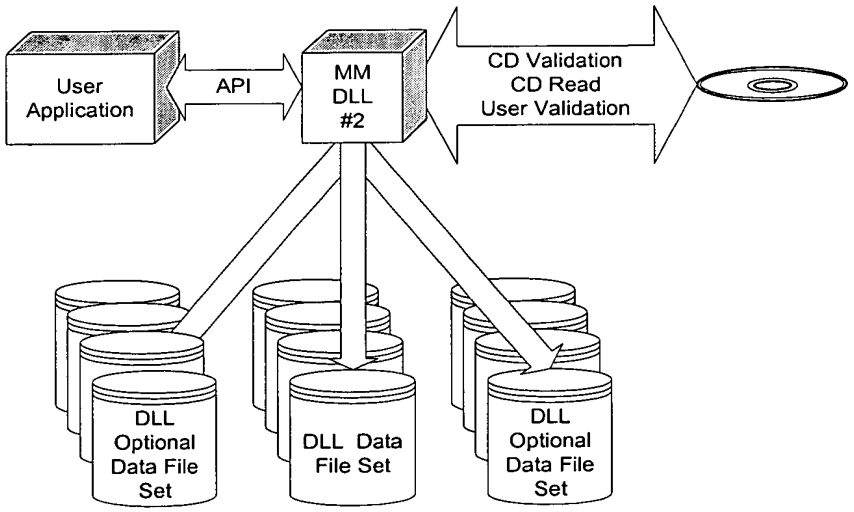
User Application
API
MM DLL #2
CD Validation
CD Read
User Validation
DLL Optional Data File Set
DLL Data File Set
DLL Optional Data File Set

FIG. 28

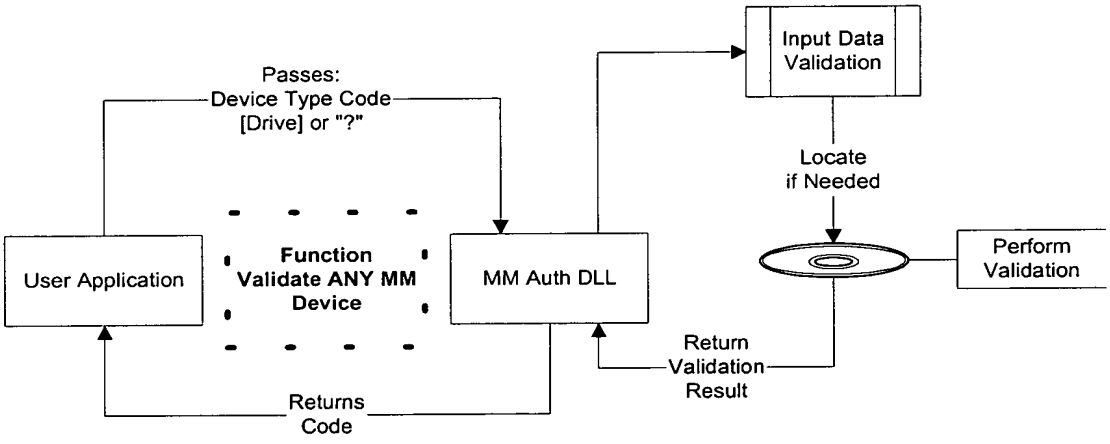
Input Data Validation
Passes:
Device Type Code
[Drive] or "?"
Locate if Needed
User Application
Function
Validate ANY MM Device
MM Auth DLL
Perform Validation
Return Validation Result
Returns Code

FIG. 29

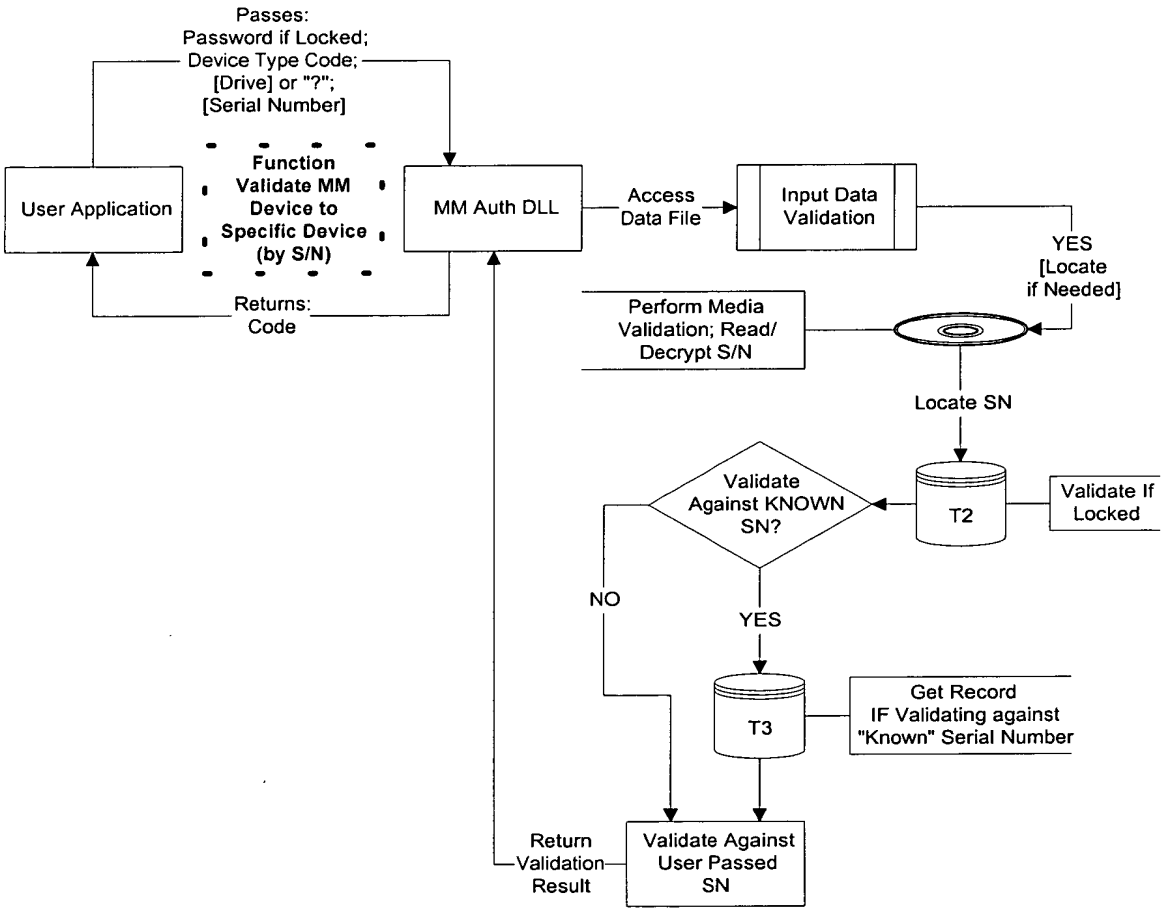
Passes:
Password if Locked;
Device Type Code;
[Drive] or "?";
[Serial Number]
User Application
Function
Validate MM
Device to
Specific Device
(by S/N)
Returns:
Code
MM Auth DLL
Access
Data File
Input Data
Validation
YES
[Locate
if Needed]
Perform Media
Validation; Read/
Decrypt S/N
Locate SN
Validate
Against KNOWN
SN?
T2
Validate If
Locked
NO
YES
T3
Get Record
IF Validating against
"Known" Serial Number
Return
Validation
Result
Validate Against
User Passed
SN

FIG. 30

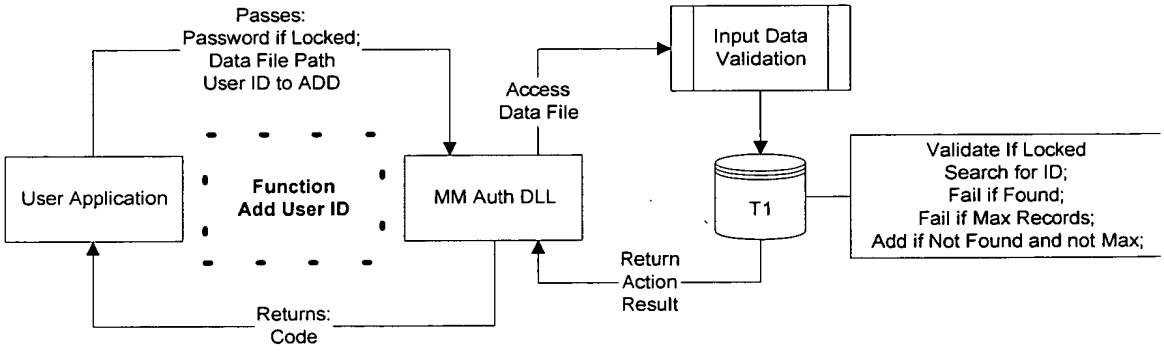
Passes:
Password if Locked;
Data File Path
User ID to ADD
User Application
Function
Add User ID
Returns:
Code
MM Auth DLL
Access
Data File
Input Data
Validation
T1
Validate If Locked
Search for ID;
Fail if Found;
Fail if Max Records;
Add if Not Found and not Max;
Return
Action
Result

FIG. 31

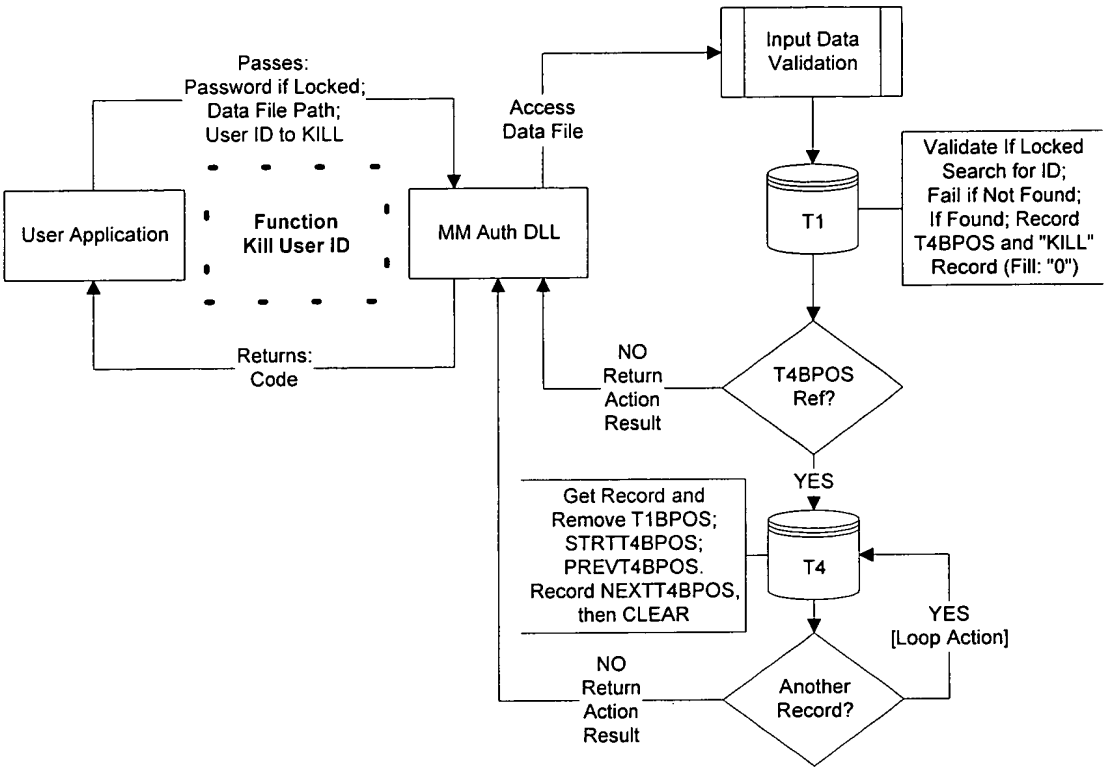

FIG. 32

Doc Code: AP.PRE.REQ
PTO/SB/33 (07-09)

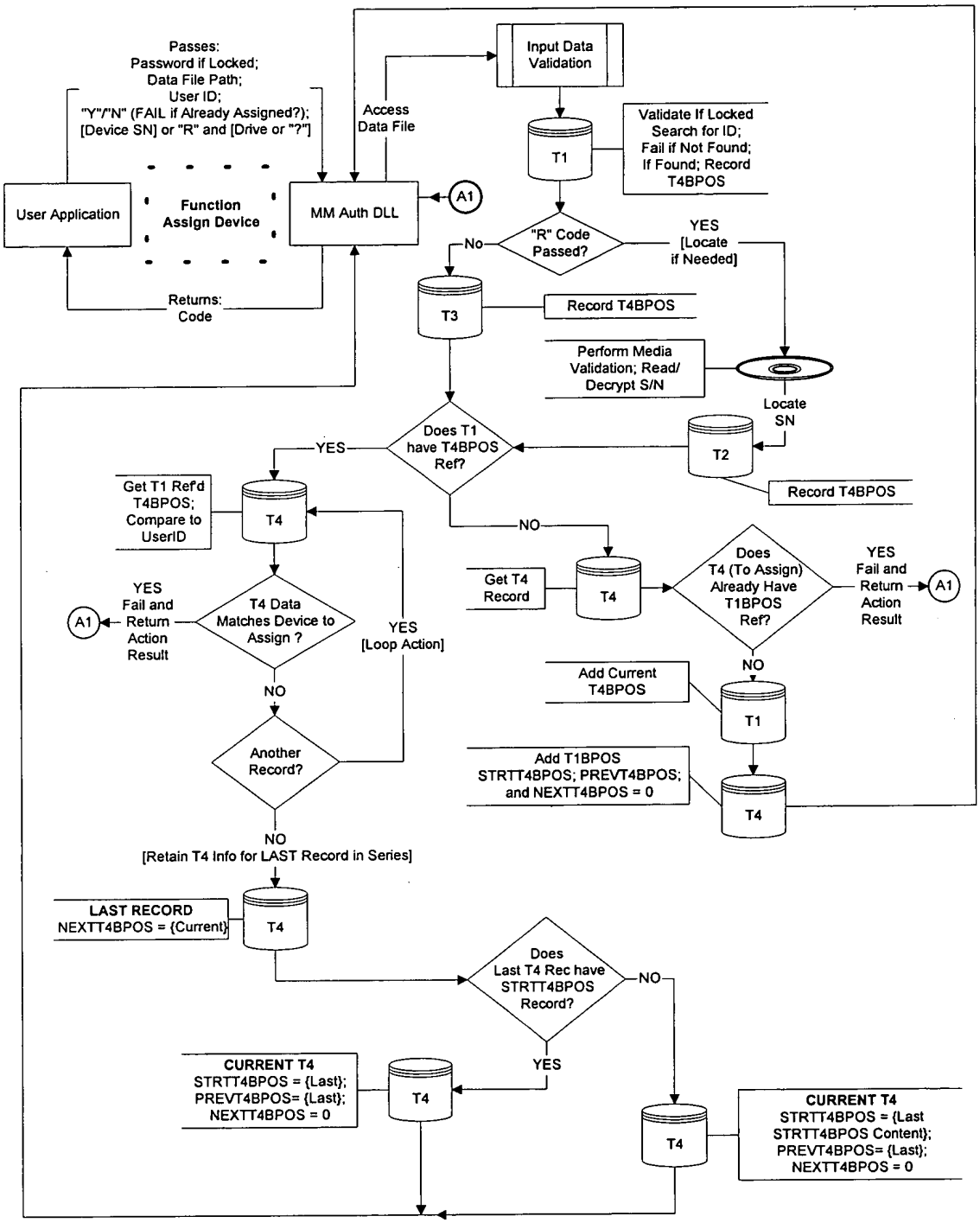
Passes:
Password if Locked;
Data File Path;
User ID;
"Y"/"N" (FAIL if Already Assigned?);
[Device SN] or "R" and [Drive or "?"]
User Application
Function
Assign Device
MM Auth DLL
A1
Access
Data File
Returns:
Code
Input Data
Validation
T1
Validate If Locked
Search for ID;
Fail if Not Found;
If Found; Record
T4BPOS
"R" Code
Passed?
No
YES
[Locate
if Needed]
T3
Record T4BPOS
Perform Media
Validation; Read/
Decrypt S/N
Locate
SN
T2
Record T4BPOS
Does T1
have T4BPOS
Ref?
YES
NO
Get T1 Ref'd
T4BPOS;
Compare to
UserID
T4
YES
Fail and
Return
Action
Result
A1
T4 Data
Matches Device to
Assign ?
YES
[Loop Action]
NO
Another
Record?
NO
[Retain T4 Info for LAST Record in Series]
Get T4
Record
T4
Does
T4 (To Assign)
Already Have
T1BPOS
Ref?
YES
Fail and
Return
Action
Result
A1
NO
Add Current
T4BPOS
T1
Add T1BPOS
STRTT4BPOS; PREVT4BPOS;
and NEXTT4BPOS = 0
T4
LAST RECORD
NEXTT4BPOS = {Current}
T4
Does
Last T4 Rec have
STRTT4BPOS
Record?
NO
YES
CURRENT T4
STRTT4BPOS = {Last};
PREVT4BPOS= {Last};
NEXTT4BPOS = 0
T4
T4
CURRENT T4
STRTT4BPOS = {Last
STRTT4BPOS Content};
PREVT4BPOS= {Last};
NEXTT4BPOS = 0

FIG. 33

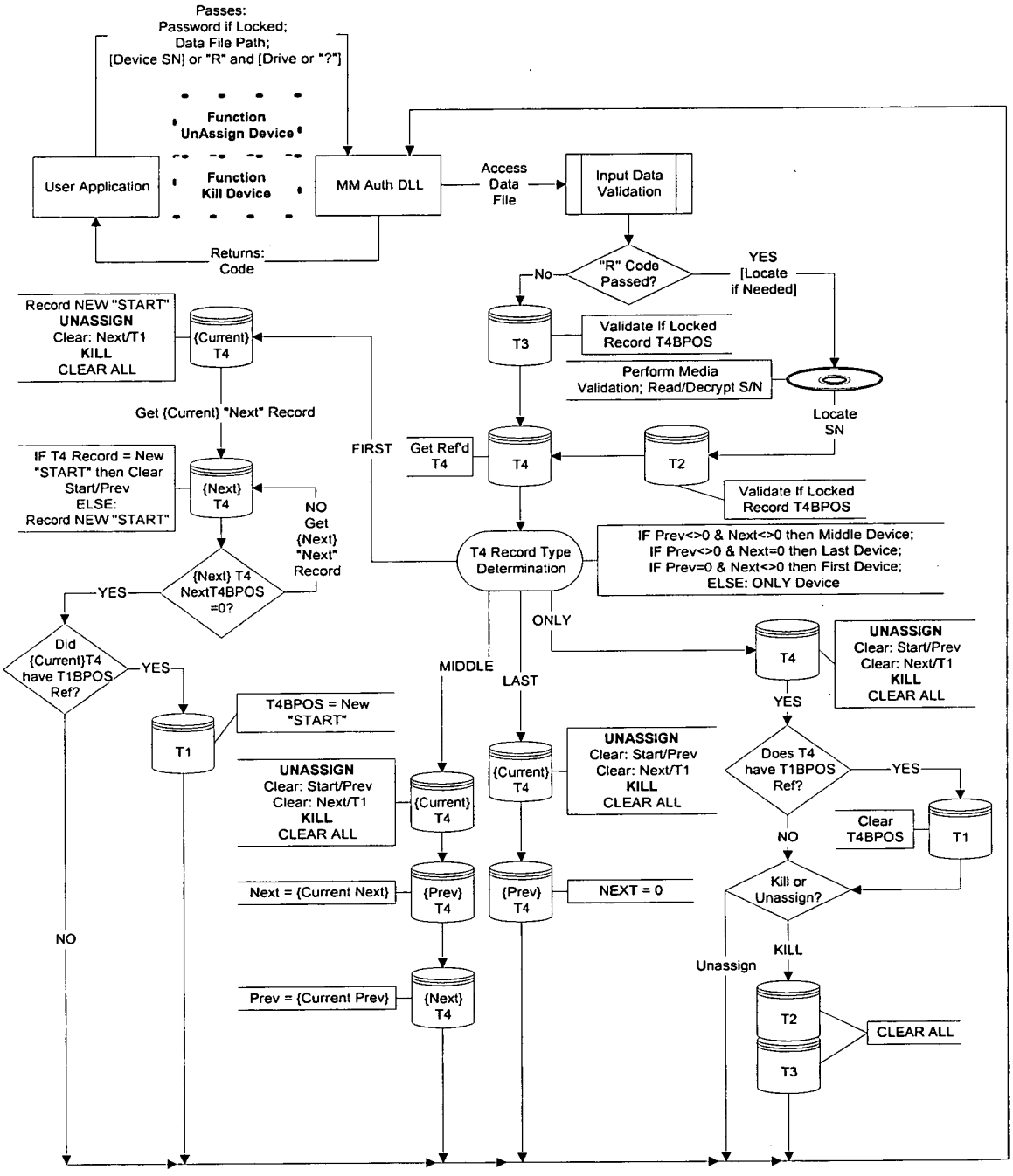
Passes:
Password if Locked;
Data File Path;
[Device SN] or "R" and [Drive or "?"]
Function UnAssign Device
Function Kill Device
User Application
MM Auth DLL
Access Data File
Input Data Validation
Returns: Code
"R" Code Passed?
No
YES [Locate if Needed]
Record NEW "START" UNASSIGN Clear: Next/T1 KILL CLEAR ALL
{Current} T4
T3
Validate If Locked Record T4BPOS
Perform Media Validation; Read/Decrypt S/N
Locate SN
Get {Current} "Next" Record
IF T4 Record = New "START" then Clear Start/Prev ELSE: Record NEW "START"
{Next} T4
FIRST
Get Ref'd T4
T4
T2
Validate If Locked Record T4BPOS
NO Get {Next} "Next" Record
T4 Record Type Determination
IF Prev<>0 & Next<>0 then Middle Device;
IF Prev<>0 & Next=0 then Last Device;
IF Prev=0 & Next<>0 then First Device;
ELSE: ONLY Device
{Next} T4 NextT4BPOS =0?
YES
ONLY
Did {Current}T4 have T1BPOS Ref?
YES
MIDDLE
LAST
T4
UNASSIGN Clear: Start/Prev Clear: Next/T1 KILL CLEAR ALL
YES
T4BPOS = New "START"
T1
UNASSIGN Clear: Start/Prev Clear: Next/T1 KILL CLEAR ALL
{Current} T4
UNASSIGN Clear: Start/Prev Clear: Next/T1 KILL CLEAR ALL
Does T4 have T1BPOS Ref?
YES
Clear T4BPOS
T1
NO
Next = {Current Next}
{Prev} T4
{Prev} T4
NEXT = 0
Kill or Unassign?
NO
KILL
Unassign
Prev = {Current Prev}
{Next} T4
T2
T3
CLEAR ALL

FIG. 34

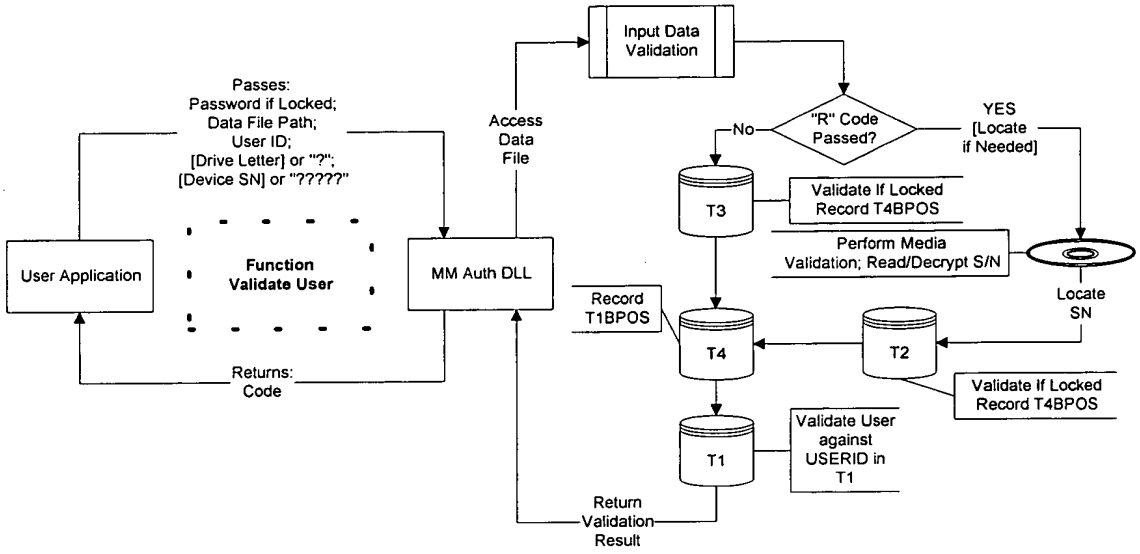
Input Data Validation
Passes:
Password if Locked;
Data File Path;
User ID;
[Drive Letter] or "?";
[Device SN] or "?????"
Access Data File
"R" Code Passed?
No
YES [Locate if Needed]
T3
Validate If Locked Record T4BPOS
Perform Media Validation; Read/Decrypt S/N
Locate SN
User Application
Function Validate User
MM Auth DLL
Record T1BPOS
T4
T2
Validate If Locked Record T4BPOS
Returns: Code
T1
Validate User against USERID in T1
Return Validation Result

FIG. 35

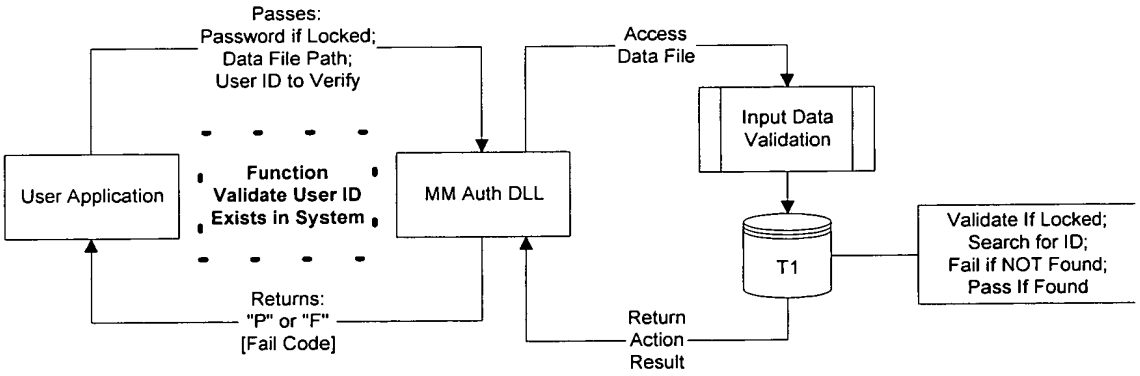
Passes:
Password if Locked;
Data File Path;
User ID to Verify
Access Data File
Input Data Validation
User Application
Function Validate User ID Exists in System
MM Auth DLL
T1
Validate If Locked; Search for ID; Fail if NOT Found; Pass If Found
Returns: "P" or "F" [Fail Code]
Return Action Result

FIG. 36

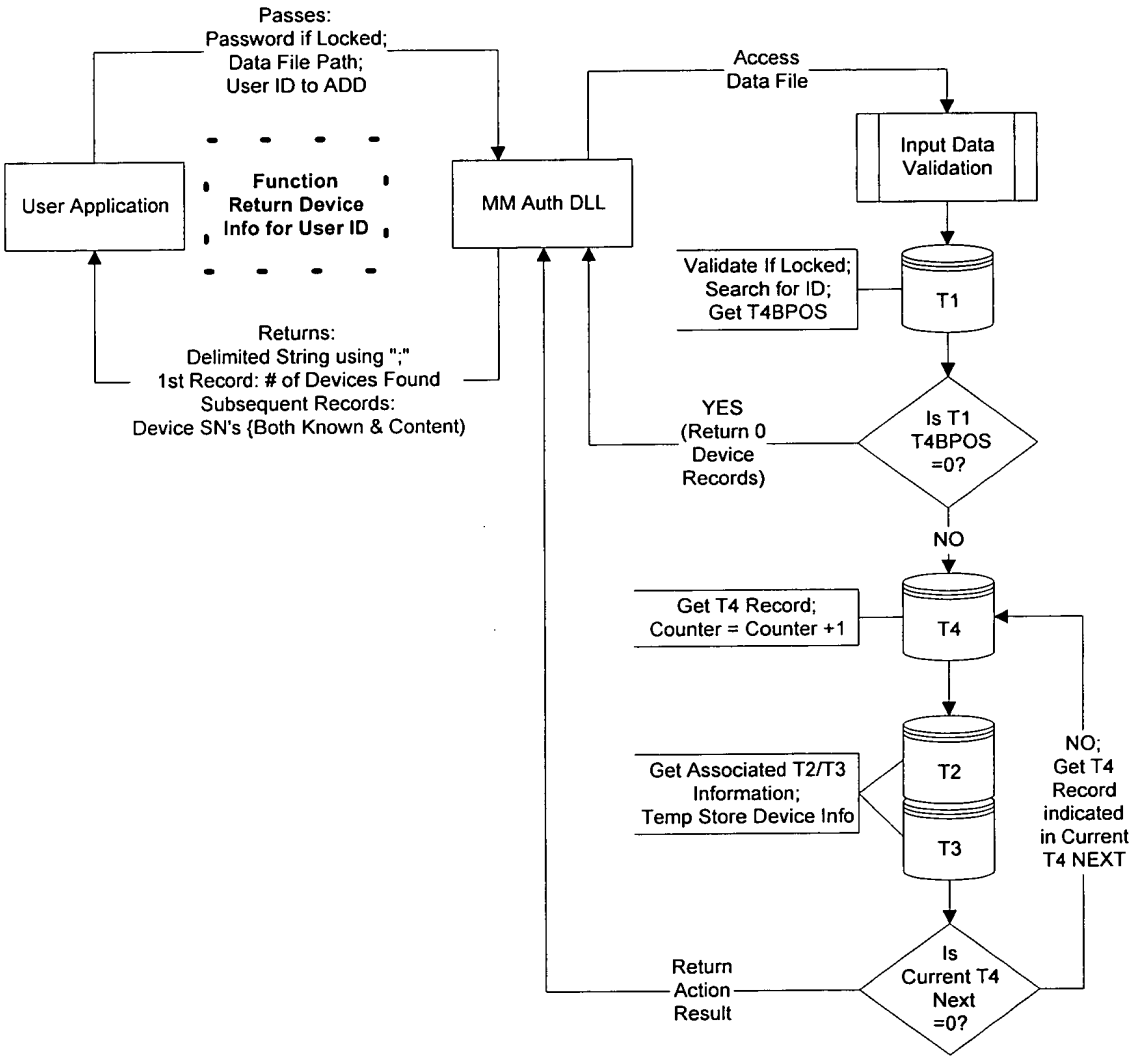
Passes:
Password if Locked;
Data File Path;
User ID to ADD
User Application
Function
Return Device
Info for User ID
Returns:
Delimited String using ";"
1st Record: # of Devices Found
Subsequent Records:
Device SN's {Both Known & Content)
MM Auth DLL
Access
Data File
Input Data
Validation
Validate If Locked;
Search for ID;
Get T4BPOS
T1
Is T1
T4BPOS
=0?
YES
(Return 0
Device
Records)
NO
Get T4 Record;
Counter = Counter +1
T4
Get Associated T2/T3
Information;
Temp Store Device Info
T2
T3
NO;
Get T4
Record
indicated
in Current
T4 NEXT
Is
Current T4
Next
=0?
Return
Action
Result

FIG. 37

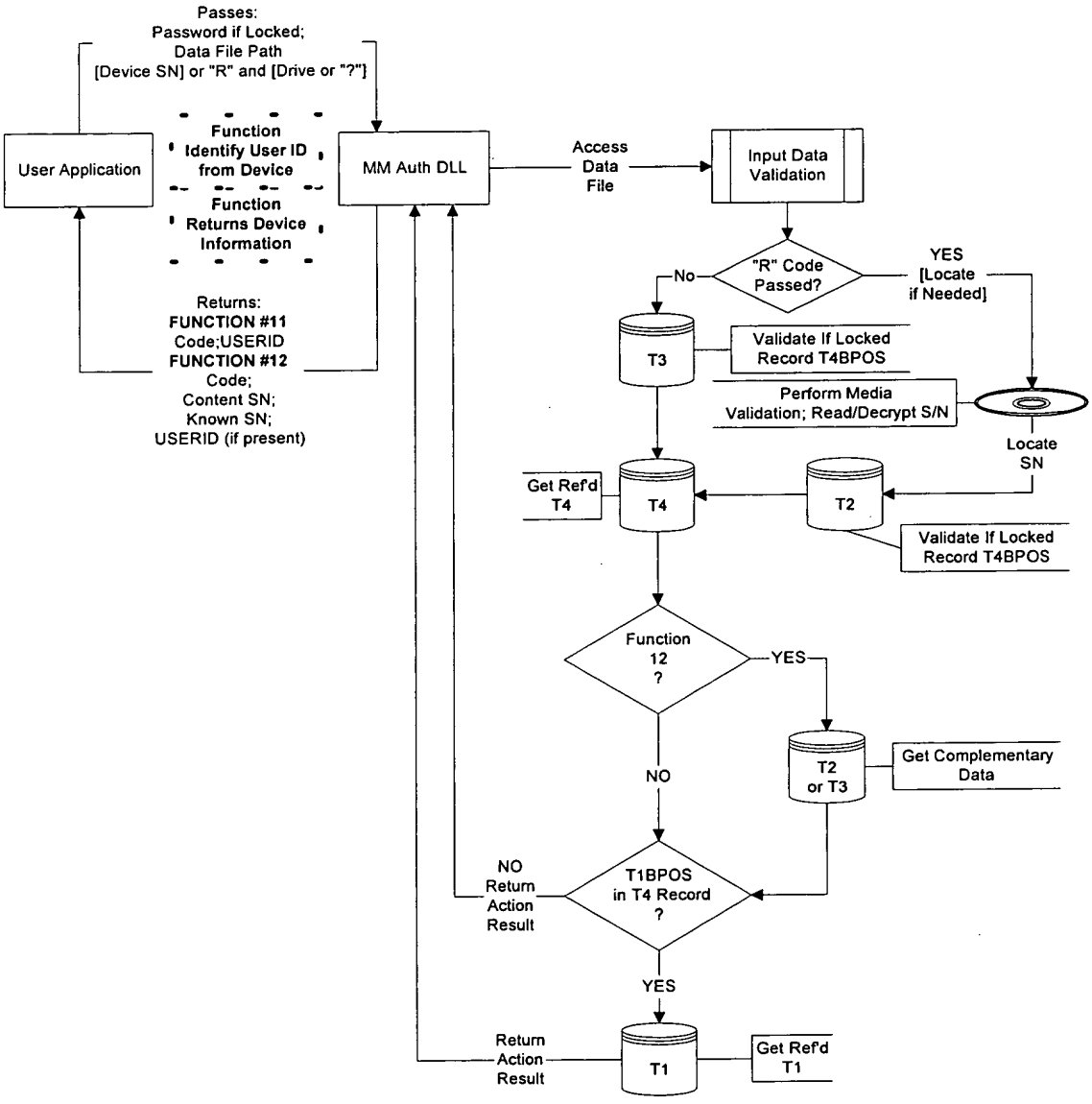
Passes:
Password if Locked;
Data File Path
[Device SN] or "R" and [Drive or "?"]
User Application
Function
Identify User ID
from Device
Function
Returns Device
Information
MM Auth DLL
Access
Data
File
Input Data
Validation
"R" Code
Passed?
No
YES
[Locate
if Needed]
Returns:
FUNCTION #11
Code;USERID
FUNCTION #12
Code;
Content SN;
Known SN;
USERID (if present)
T3
Validate If Locked
Record T4BPOS
Perform Media
Validation; Read/Decrypt S/N
Locate
SN
Get Ref'd
T4
T4
T2
Validate If Locked
Record T4BPOS
Function
12
?
YES
NO
T2
or T3
Get Complementary
Data
NO
Return
Action
Result
T1BPOS
in T4 Record
?
YES
Return
Action
Result
T1
Get Ref'd
T1

FIG. 38

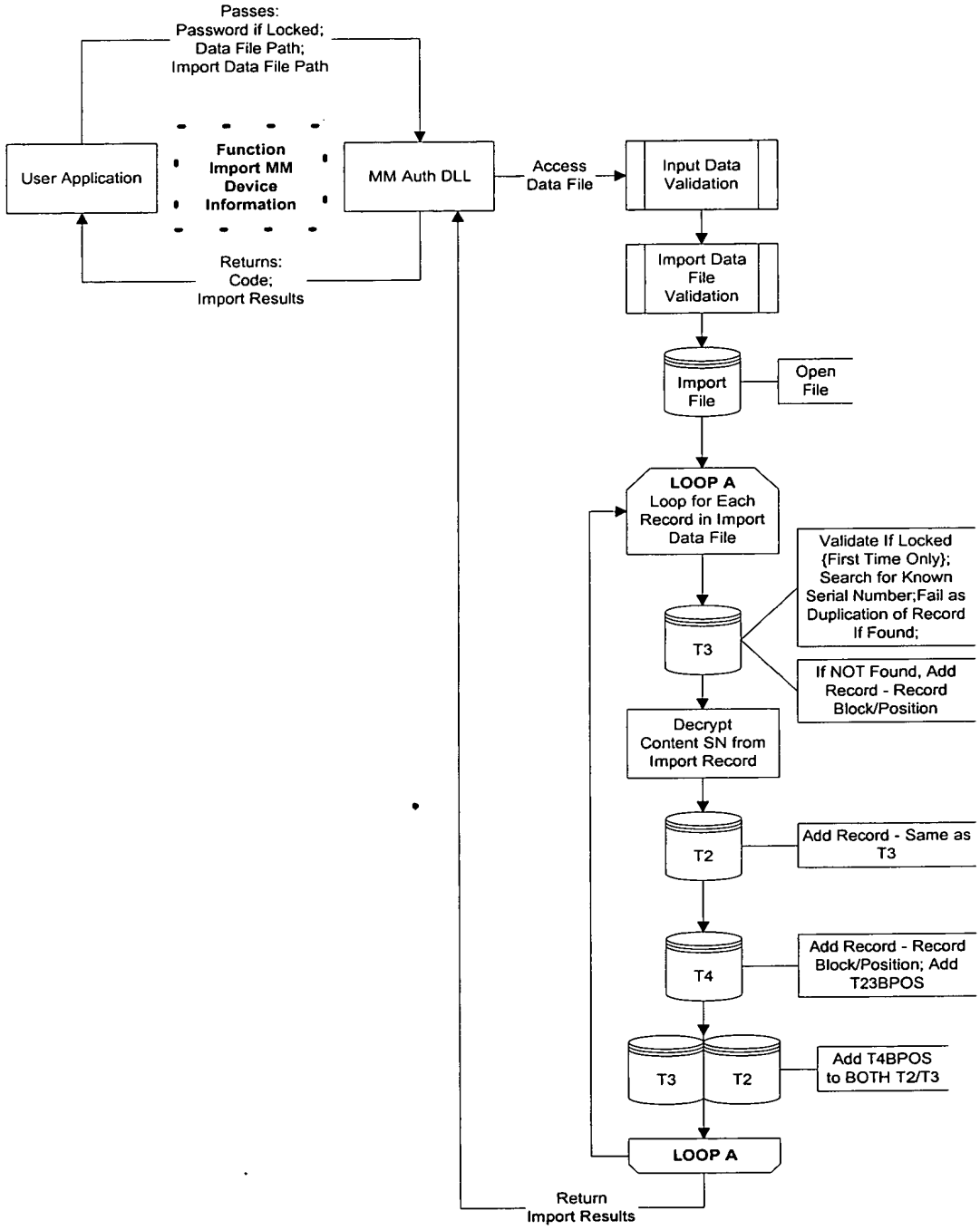
Passes:
Password if Locked;
Data File Path;
Import Data File Path
User Application
Function
Import MM
Device
Information
MM Auth DLL
Access
Data File
Input Data
Validation
Import Data
File
Validation
Import
File
Open
File
LOOP A
Loop for Each
Record in Import
Data File
Validate If Locked
{First Time Only};
Search for Known
Serial Number;Fail as
Duplication of Record
If Found;
T3
If NOT Found, Add
Record - Record
Block/Position
Decrypt
Content SN from
Import Record
T2
Add Record - Same as
T3
T4
Add Record - Record
Block/Position; Add
T23BPOS
T3
T2
Add T4BPOS
to BOTH T2/T3
LOOP A
Returns:
Code;
Import Results
Return
Import Results

FIG. 39

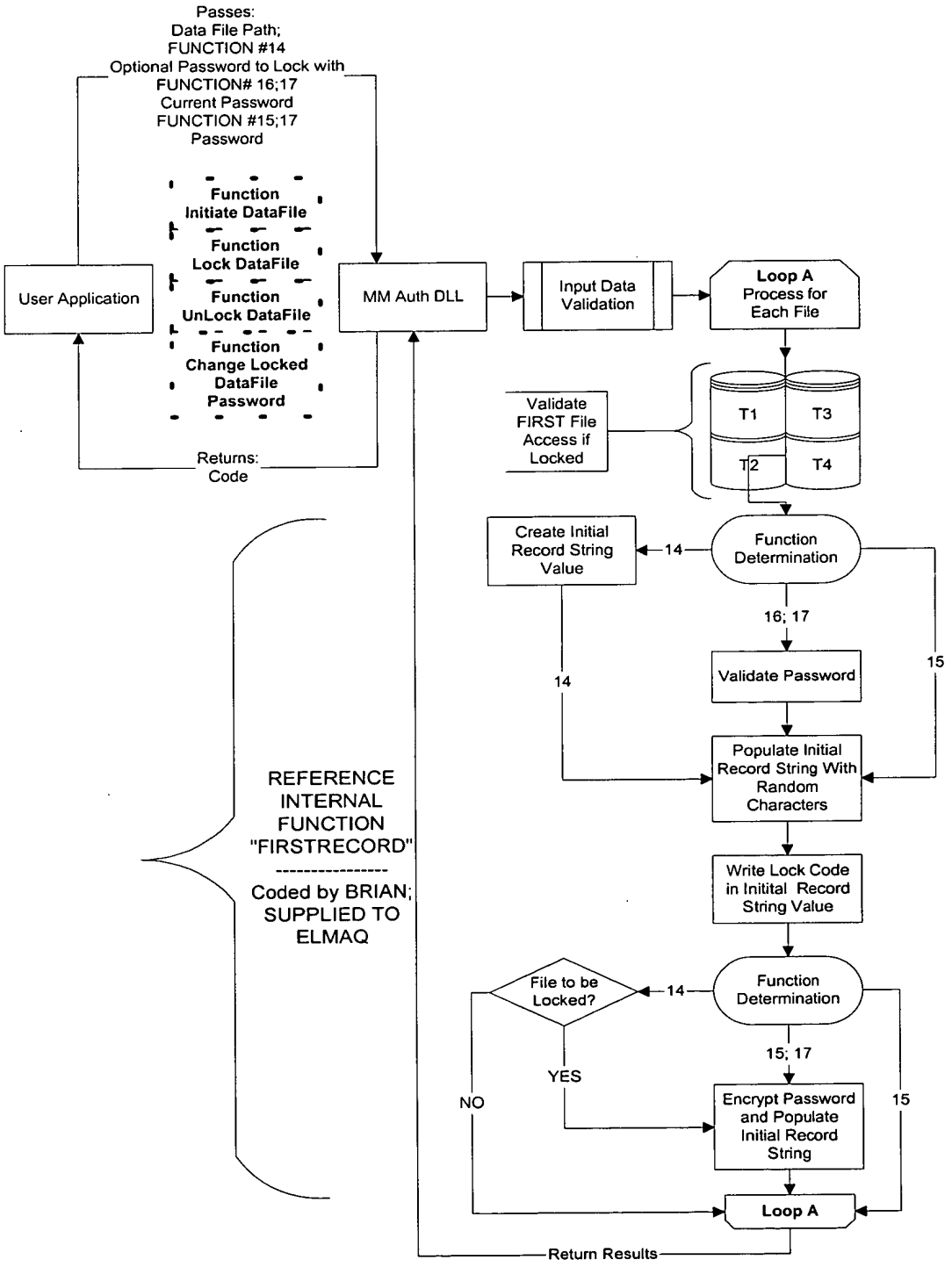
Passes:
Data File Path;
FUNCTION #14
Optional Password to Lock with
FUNCTION# 16;17
Current Password
FUNCTION #15;17
Password
Function Initiate DataFile
Function Lock DataFile
Function UnLock DataFile
Function Change Locked DataFile Password
User Application
MM Auth DLL
Input Data Validation
Loop A Process for Each File
Returns:
Code
Validate FIRST File Access if Locked
T1
T3
T2
T4
Create Initial Record String Value
14
Function Determination
16; 17
15
14
Validate Password
Populate Initial Record String With Random Characters
REFERENCE INTERNAL FUNCTION "FIRSTRECORD"
Coded by BRIAN; SUPPLIED TO ELMAQ
Write Lock Code in Initital Record String Value
File to be Locked?
14
Function Determination
15; 17
YES
NO
Encrypt Password and Populate Initial Record String
15
Loop A
Return Results

FIG. 40

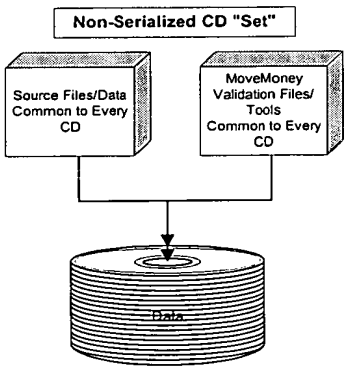
Non-Serialized CD "Set"
Source Files/Data Common to Every CD
MoveMoney Validation Files/ Tools Common to Every CD
Data

FIG. 41

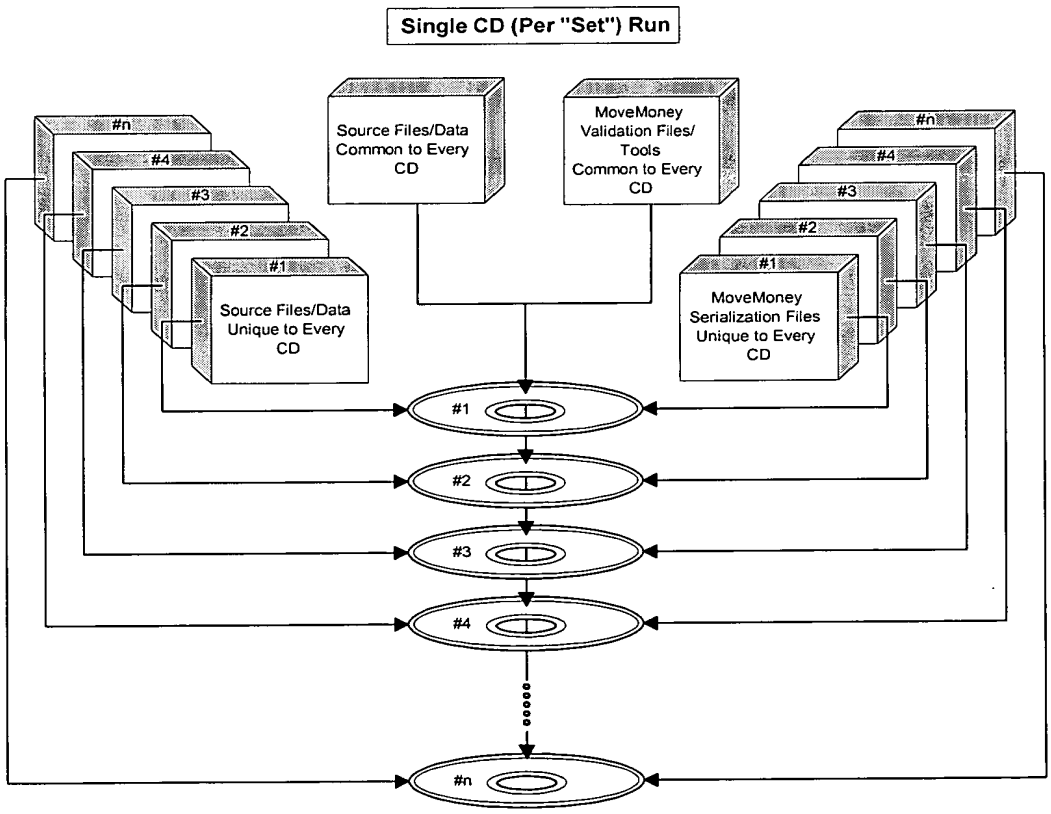
Single CD (Per "Set") Run
Source Files/Data Common to Every CD
MoveMoney Validation Files/ Tools Common to Every CD
#n
#4
#3
#2
#1
Source Files/Data Unique to Every CD
MoveMoney Serialization Files Unique to Every CD

FIG. 42

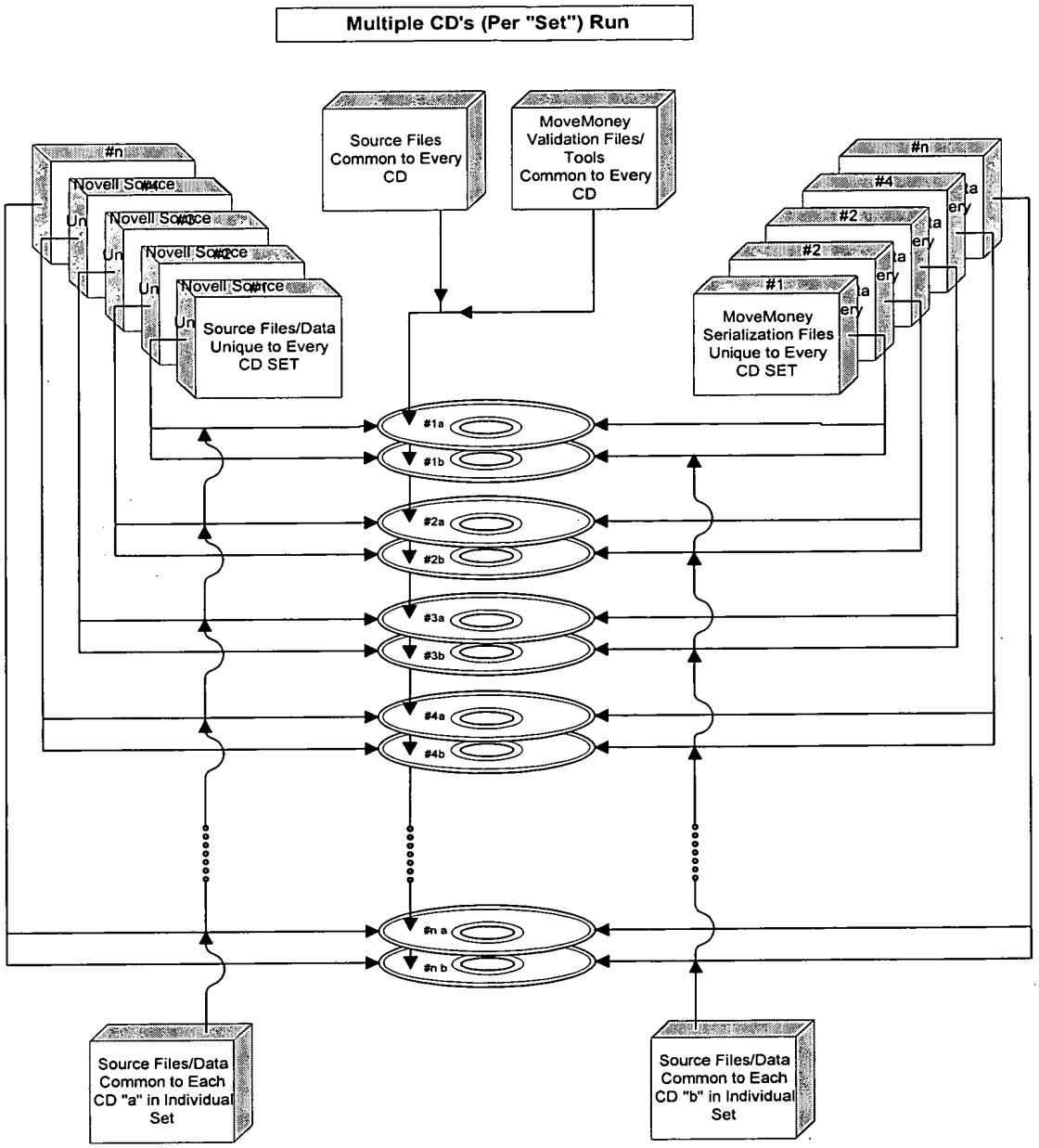
Multiple CD's (Per "Set") Run
Source Files Common to Every CD
MoveMoney Validation Files/ Tools Common to Every CD
Source Files/Data Unique to Every CD SET
MoveMoney Serialization Files Unique to Every CD SET
#1a
#1b
#2a
#2b
#3a
#3b
#4a
#4b
#n a
#n b
Source Files/Data Common to Each CD "a" in Individual Set
Source Files/Data Common to Each CD "b" in Individual Set

FIG. 43

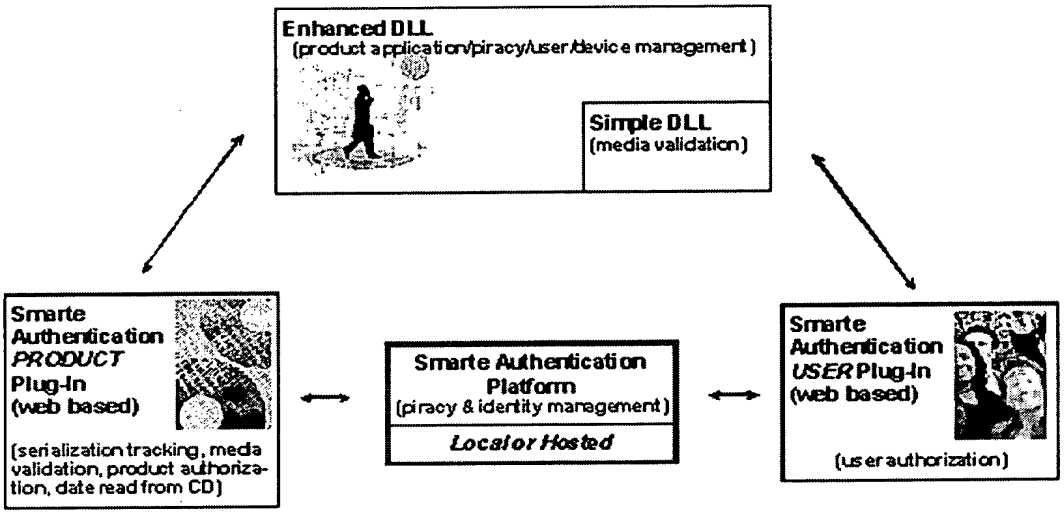
Enhanced DLL
(product application/piracy/user/device management)
Simple DLL
(media validation)
Smarte Authentication PRODUCT Plug-In (web based)
(serialization tracking, media validation, product authorization, date read from CD)
Smarte Authentication Platform
(piracy & identity management)
Local or Hosted
Smarte Authentication USER Plug-In (web based)
(user authorization)

FIG. 44